3. Tätigkeitsbericht des Diözesandatenschutzbeauftragten der ostdeutschen Bistümer und des Katholischen Militärbischofs

gemäß § 18 Abs. 3 KDO und

gemäß § 44 Abs. 6 KDG

Berichtszeitraum 01.01.2018 bis 31.12.2018

"Zu argumentieren, dass man sich nicht um das Recht auf Privatsphäre schert, weil man nichts zu verbergen habe, ist nichts anderes, als wenn man konstatiert, dass man sich nicht um freie Meinungsäußerung schert, weil man nichts zu sagen hat.“

Edward Snowden

3. Tätigkeitsbericht des Diözesandatenschutzbeauftragten für

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

Inhaltsverzeichnis

Abkürzungsverzeichnis

AG	Amtsgericht
ArbG	Arbeitsgericht
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidung des Bundesgerichtshofes im Zivilsachen
BT-Drs	Buntestag Drucksache
BVerfGE	Bundesverfassungsgerichtsentscheidung
BZRG	Bundeszentralregister
CR	Computer und Recht (Zeitschrift)
DKWW	Däubler, Klebe, Wedde, Weichert
DSG-EKD	Datenschutzgesetz der Evangelischen Kirche
DSGVO	Datenschutzgrundverordnung
EuDSRL	Europäische Datenschutzrichtlinie
EuGH	Europäischer Gerichtshof
DuD	Datenschutz und Datensicherheit
GG	Grundgesetz
JGG	Jugendgerichtsgesetz
KDO	Kirchliche Datenschutzordnung
KDG	Kirchrchliches Datenschutzgesetz
KDR-OG	Kirchl. Datenschutzregelung der Ordensgemeinschaft päpstl. Rechts
KUG	Kunsturhebergesetz
LbfDI/LfD	Landesbeauftragter für Datenschutz und Informationsfreiheit
LG	Landgericht

LAG	Landesarbeitsgericht
NJW	Neue Juristische Wochenschrift
NZA	Neue Zeitschrift für Arbeitsrecht
OLG	Oberlandesgericht
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
UrhG	Urhebergesetz
VG	Verwaltungsgericht
WR	Weimarer Rebublik
ZD	Zeitschrift für Datenschutz

Vorwort

Big Data ist längst kein Begriff mehr, der eine Zukunftsvision beschreibt. Jeden Tag kommen Mitbürger*innen in Kontakt mit IT gestützten Verarbeitungsprozessen. Ohne die Nutzung eines Internet-Anschlusses sind häufig auch alltägliche Prozesse nicht zu bewältigen. Das betrifft nicht nur Bestellung bei kommerziellen Anbietern, sondern auch die Inanspruchnahme von Dienstleistungen und Auskünften von Behörden.

Über Apps können Haushaltsfunktionen gesteuert werden und smarte Haushaltsgeräte können die Zutaten für das über das Internet ausgewählte Essen direkt beim Handel bestellen, der diese dann ins Haus liefert.

Damit einher geht die Bereitschaft, Entscheidungen von technischen Einrichtungen zu fällen oder zumindest maßgeblich beeinträchtigen zu lassen. Das betrifft Entscheidungsprozesse bei der Einstellung von Bewerbern auf einen Arbeitsplatz, die Kreditvergabe, aber auch die Partnerwahl über entsprechende Börsen.

Durch diese Entwicklung wächst die Konzentration von vor allem auch personenbezogenen Daten bei großen Unternehmen ständig an. Die Macht solcher Unternehmen über solche Informationen Personalprofile erstellen zu können, birgt zunehmend eine Gefahr für die Demokratie. Datenschutz dient der Wahrung des Grundrechts eines jeden einzelnen auf informationelle Selbstbestimmung und ist damit Voraussetzung für Datensouveränität.

Gleichzeitig dient Datenschutz dadurch der Funktionsfähigkeit des Staates.

1. Einleitung

1.1. Einführung der DSGVO

Die Einführung der Europäischen Datenschutzgrundverordnung (DSGVO) zum 25. Mai 2018 war über lange Zeit hinweg das beherrschende Thema in der Presse. Dabei wurde häufig der Eindruck erweckt, etwas revolutionär Neues wird den Bürgern von der Europäischen Union aufgedrückt. Bei näherer Betrachtung hätte jedoch ein Jeder schnell feststellen können, dass die Vorschriften des europäisch einheitlichen Regelwerkes bereits zuvor im Bundesdatenschutzgesetz verankert und damit auch vor dem Inkrafttreten der DSGVO geltendes Recht in der Bundesrepublik gewesen sind.

Datenschutz und Privatsphäre werden auch weiterhin zu den Top-Themen des Jahrhunderts gehören.[1]Mit der DSGVO hat die EU einen datenschutzrechtlichen Standard etabliert, der auch international anerkannt wird.[2]

Leider wurden im Rahmen der Einführung der Verordnung von zahlreichen interessierten Stellen kompromittierende Ausführungen in die Öffentlichkeit gebracht, die den Datenschutz lächerlich machen oder/und die Bürger verunsichern sollten. So war die Aufregung groß, als eine Wohnungsbaugesellschaft in Wien sich verpflichtet sah, die Klingelschilder mit Namensaufdruck zu entfernen, was datenschutzrechtlich keinesfalls veranlasst war, so aber in die Öffentlichkeit lanciert wurde. Ebenfalls für Aufsehen sorgte das Vorgehen eines katholischen Kindergartens, der in seinem mit Bildern versehenen Jahresbericht die Gesichter der Kinder schwärzte. Derartige Legenden und Pseudo-Skandale sind vor allem dazu geeignet, gegenüber einem modernen Datenschutz eine negative Grundstimmung zu erzeugen. Die Digitalisierung steht erst am Anfang und wird künftig immer mehr Lebensbereiche erfassen. Künstliche Intelligenz, biometrische Überwachung und social scoring benennen nur einige Bereiche mit denen ein tiefer Eingriff in die Persönlichkeitsrechte des Einzelnen möglich ist. Der Respekt vor der Freiheit des Einzelnen auf Schutz seiner Persönlichkeit, insbesondere seine Intimsphäre, ist Bestandteil des christlichen Menschenbildes.[3] Digitalisierung und Datenschutz dürfen nicht gegeneinander ausgespielt werden. Damit die Digitalisierung dem Menschen dient, muss der Datenschutz dafür sorgen, dass seine Grundrechte gewahrt bleiben.

[1] Presseerklärung zum 27. TB HmbBfDI vom 21.02.2019
[2] Durch von der EU erlassene Angemessenheitsbeschlüsse ist ein Datentransfer auch in die benannten Länder außerhalb des europäischen Wirtschaftsraums möglich.
[3]Tipps aus der kirchlichen Meldestelle Berufsverband der Pfarrsekretärinnen und Pfarrsekretäre der Erzdiözese Freiburg

1.2. Einführung des KDG

Die Arbeit in diesem Jahr wurde maßgeblich von der Einführung des neuen KDG bestimmt. Dabei erwies sich die enge Personalsituation einmal mehr als problematisch. In den fünf Bistümern wurden im Berichtsjahr ca. 50 Vorträge zum Datenschutz und zum neuen KDG gehalten. Die Teilnehmerzahlen der einzelnen Veranstaltungen lagen zwischen 12 und 200 Teilnehmern. So konnten direkt durch die Vortragstätigkeit ca. 2.500 Personen direkt mit den neuen gesetzlichen Regelungen vertraut gemacht werden. Die Zuhörer stammten dabei wesentlich aus dem Bereich der hauptamtlichen Mitarbeiter. Aber vor allem bei den Abendveranstaltungen konnte ein großer Anteil ehrenamtlich Tätiger in der Kirche begrüßt werden.

Weiterhin wurde das Kirchliche Datenschutzrecht mit den Vorsitzenden der Regierungsfraktionen im Landtag von Sachsen-Anhalt (CDU, Grüne, SPD) besprochen. Ebenso wurden diesbezügliche Gespräche mit dem Innenpolitischen Sprecher der SPD-Fraktion im Deutschen Bundestag und dem Innenminister von Sachsen-Anhalt geführt.

Neben den Schulungen werden weiterhin regelmäßig Arbeitskreise zum Erfahrungsaustausch mit den betrieblichen Datenschutzbeauftragten veranstaltet. Diese dienen dazu, den betrieblichen Datenschutzbeauftragten die Möglichkeit zu geben, Fragen oder Probleme, die in ihrem Bereich aufgetreten sind mit anderen betrieblichen Datenschutzbeauftragten und der Datenschutzaufsicht zu besprechen. Diese Erfahrungsaustauschkreise werden von den betreffenden Datenschutzbeauftragten umfangreich angenommen und eingefordert. Perspektivisch sollen solche Kreise auch für die betrieblichen Datenschutzbeauftragten der Pfarreien eingerichtet werden. Das Angebot richtet sich dabei gleichermaßen an interne und externe betriebliche Datenschutzbeauftragte.

1.3. Entscheidung kirchlicher Einrichtungen DSGVO und BDSG anstelle des KDG anzuwenden

§ 3 Abs. 1 KDG legt den organisatorischen Geltungsbereich des Gesetzes fest. Dennoch gibt es Rechtsträger, die für ihren Bereich die Geltung der DSGVO anstelle des KDG reklamieren.[4]

[4]Z. B. „Tag des Herrn“ Benno Verlag siehe dort auf der Homepage Datenschutzerklärung

Dazu stellt Herr Professor Dr. Sydow in einem Vermerk vom 16.08.2018 zur Vollstreckung kirchlicher Bußgeldbescheide u. a. fest: *„Eine Regelung zum Anwendungsbereich des KDG in den Einleitungsnormen des KDG ist … möglich und empfehlenswert. Sie trägt aber immer nur so weit, wie die kirchliche Rechtsetzungsbefugnis dem Dritten gegenüber bereits vorher gegeben und im staatlichen Rechtskreis anerkannt war. … Zur Vermeidung etwaiger Streitigkeiten über die Geltung des KDG ist es deshalb sehr zu empfehlen, dass die kirchlichen Rechtsträger die Geltung des KDG in ihren eigenen Statuten festschreiben."*[5]

Sollte es kirchlichen Einrichtungen freigestellt werden, sich für die Geltung der einen oder der anderen Norm zu entscheiden, führt dies zunächst zu Rechtsunsicherheit, da dem Rechtsanwender nicht mehr klar ist, an welche Aufsicht er sich ggf. zu wenden hat. Aber auch die Aufsicht kann nicht aufgrund der Kirchlichkeit der Einrichtung sicher ihre Zuständigkeit bestimmen. Darüber hinaus wird aber das System insgesamt infrage gestellt. Bereits jetzt gibt es staatliche Datenschutzaufsichten, die das Kirchliche Datenschutzrecht auf den „Verkündigungsbereich" beschränken wollen und den Diözesandatenschutzbeauftragten eine darüber hinausgehende Zuständigkeit absprechen.[6] Fraglich erscheint auch, ob ein Wechsel von dem einen in den anderen Rechtsbereich möglich sein soll, evtl. auch ein erneuter Wechsel. Hier erscheint eine definitive Klarstellung der Bistumsleitungen erforderlich, die festlegt, dass alle Einrichtungen die der Jurisdiktion des jeweiligen Ortsordinarius unterliegen sowie Einrichtungen, die sich mehrheitlich im Eigentum einer kirchlichen juristischen Person befinden, das KDG anzuwenden haben.

2. Datenschutzaufsicht und Zuständigkeiten

2.1. Stellung der Datenschutzaufsicht

Bereits mehrfach wurde darauf hingewiesen, dass die Katholische Kirche von dem ihr aus Artikel 91 DSGVO und den Artikeln 140 GG 137 WRV eingeräumten Recht Gebrauch gemacht hat, eigene umfassende Regeln zum Datenschutz anzuwenden. Dies umfasst auch die Etablierung einer eigenen Datenschutzaufsicht in Form der Diözesandatenschutzbeauftragten. In weiten Teilen der Rechtsverpflichteten ist die Stellung dieser Dienststelle aber nicht hinreichend bekannt. So ist in der

[5]Sydow, Vermerk (Entwurf) zu Einzelfragen der Neuregelung des kirchlichen Datenschutzrechts
[6] Siehe zu diesem Thema 2. TB 2017 Punkt 3.

aufsichtlichen Tätigkeit häufig festzustellen, dass die Stellungnahmen des Diözesandatenschutzbeauftragten als die Empfehlungen eines Beraters wahrgenommen werden. In der Folge glaubt die Einrichtung dann abwägen zu können, ob sie der vermeintlichen Empfehlung Folge leistet oder nicht. An dieser Stelle ist nachhaltig auf die Regelung des § 47 KDG zu verweisen, die mit der Regelung des § 51 KDG im Zusammenhang steht. Da Artikel 91 DSGVO den Religionsgemeinschaften das Recht eigener Datenschutzregelungen nur gewährt, wenn diese mit dem EU-Recht in Einklang stehen, ist die Kirchliche Aufsicht verpflichtet für die konsequente Umsetzung des KDG zu sorgen, um diesen Einklang zu gewährleisten.

Die Anweisungen der Diözesandatenschutzbeauftragten sind damit für die Empfänger verbindlich. Soweit die Empfänger gegen die Anweisungen vorgehen möchten, steht ihnen der Rechtsweg zu den Kirchlichen Datenschutzgerichten offen.

An dieser Stelle wäre eine Verdeutlichung der Aufgaben des Diözesandatenschutzbeauftragten durch die Leitungen der Bistümer wünschenswert.

2.2. Konferenz der Diözesandatenschutzbeauftragten

Bereits im letzten Tätigkeitsbericht wurde die Gründung der Konferenz der Diözesandatenschutzbeauftragten dargestellt.[7]

Die Konferenz der Diözesandatenschutzbeauftragten tagt in regelmäßigen Abständen. Darüber hinaus gibt es zahlreiche weitere Abstimmungen nicht zuletzt um die inzwischen 15 von den Teilnehmern der Konferenz erarbeiteten Praxishilfen zum KDG zu erstellen, die auf den Homepages der Diözesandatenschutzbeauftragten einheitlich unter gemeinsamem Logo veröffentlicht sind.

Nachdem die Konferenz in den vergangenen Monaten auch mehrere Beschlüsse gefasst und veröffentlicht hat, wurde mehrfach die Frage nach der Kompetenz der Konferenz und der Verbindlichkeit ihrer Beschlüsse gefragt. Nach § 44 Abs. 3 lit. f) KDG gehört es zu den Aufgaben des Diözesandatenschutzbeauftragten, *“mit anderen Datenschutzaufsichten zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes zu gewährleisten.“* Vor diesem Hintergrund treffen sich die Diözesandatenschutzbeauftragten in regelmäßigen Abständen, um die einheitliche Anwendung des KDG sicherzustellen. Diese Treffen finden unter der Bezeichnung „Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche

[7] 2. TB 2017 Seite 16

Deutschland“ statt. Die von der Konferenz der Diözesandatenschutzbeauftragten gefassten Beschlüsse geben die Rechtsauffassung der Diözesandatenschutzbeauftragten wieder. Sie stellen somit eine verbindliche Auslegung der Regelungen des KDG dar, gegen die die dem KDG verpflichteten Einrichtungen und Personen im konkreten Fall durch Anrufung des kirchlichen Datenschutzgerichtes vorgehen können. Durch die Beschlüsse soll also dem Rechtsanwender zunächst eine praktische Hilfe an die Hand gegeben werden, um ihm eine sichere Anwendung der datenschutzrechtlichen Normen zu ermöglichen.

Bedauerlicher Weise wurden einige Beschlüsse in der katholischen Presse, insbesondere von einem Online-Organ, massiv kritisiert. Dabei wurde der Eindruck erweckt, der Datenschutz behindere die Wahrnehmung einer zeitgemäßen Verkündigung. Selbstverständlich steht auch der katholischen Presse die Pressefreiheit gegenüber den Aufsichtsorganen der Katholischen Kirche zu. Wünschenswert wäre es jedoch eine sachliche und problemorientierte Auseinandersetzung zu führen, bei der den Datenschutzaufsichten kompetente Journalisten gegenüberstehen, die das Thema Datenschutz verantwortungsvoll bearbeiten. Kritik, welche schlicht die oft unreflektierten und unberechtigten Besorgnisse von Betroffenen wiedergibt, ist weder dem Ansehen der katholischen Presse noch dem des Datenschutzes zuträglich.

2.3. Diözesandatenschutzbeauftragte ./. Ordensdatenschutzbeauftragte der Orden päpstlichen Rechts

Das KDG gilt zunächst nur für die Einrichtungen der Diözesen, deren Ortsbischof diese Regelung für das betreffende Bistum in Kraft gesetzt hat. Für die Orden päpstlichen Rechts ist dies aufgrund der Regelung des Can 381 § 1 C.I.C. nicht möglich. Für die Orden päpstlichen Rechts gilt nicht das KDG, sondern das KDR-OG. Damit sind Einrichtungen im Bereich der Ordensgemeinschaft päpstlichen Rechts und im Bereich der von dieser ganz oder mehrheitlich getragenen Werke und Einrichtungen, ohne Rücksicht auf deren zivilen Rechtsformen, der Aufsicht des Diözesandatenschutzbeauftragten entzogen.[8]

Durch diese Regelungen kommt zusätzliche Rechtsunsicherheit auf. Zum einen mit den staatlichen Datenschutzaufsichten der Länder, die regelmäßig Eingaben, die kirchlichen Einrichtungen betreffen, an die Diözesandatenschutzbeauftragen

[8] § 3 Abs.1 KDR-OG

weiterleiten, zum anderen aber auch unter den kirchlichen Datenschutzaufsichten. So ist nicht aufgrund der Belegenheit der Einrichtung erkennbar, welchem Recht diese unterliegt. Häufig sind die jeweiligen Einrichtungen „Unter-“ oder „Unter-Untereinrichtungen“ des jeweiligen Ordens päpstlichen Rechts.

Auch die Einrichtungen selber scheinen sich nicht in jedem Fall über das für sie geltende Recht im Klaren zu sein.

Fraglich ist zudem auch die organisatorische Ausstattung der Datenschutzaufsichten. Hier sind wenige Personen für das gesamte Bundesgebiet zuständig. Eine eindeutige Übersicht, welcher Orden päpstlichen Rechts durch welche Datenschutzaufsicht betreut wird, fehlt.

Die in § 43 Abs. 2 KDG verankerte Regelung, wonach der Diözesandatenschutzbeauftragte sein Amt hauptamtlich ausübt, erfährt in § 43 Abs. 2 KDR-OG eine Aufweichung, weil danach der Ordensdatenschutzbeauftragte sein Amt nur „in der Regel“ hauptamtlich ausüben soll. Nach der Wahrnehmung der hiesigen Dienststelle scheint es aber tatsächlich so zu sein, dass „in der Regel“ die Datenschutzaufsicht nebenamtlich ausgeübt wird.

Soweit die Aufsicht nebenamtlich insbesondere durch hauptamtliche Rechtsanwälte ausgeübt wird, ist zu prüfen, ob Interessenkollisionen mit der anwaltlichen Beratung und aufsichtlicher Anweisung ausgeschlossen wird.

3. Datenschutzbeauftragter

3.1. Datenschutzbeauftragter ./. Datenschutzkoordinator

Neu im KDG geregelt ist die Vorschrift zu den betrieblichen Datenschutzbeauftragten. Diese sind zunächst in allen Einrichtungen gem. § 3 Abs. 1 KDG zu bestellen, unabhängig von deren personeller Ausstattung oder anderen quantitativen Merkmalen. Dies betrifft vor allem die Pfarreien.

Auch ist nunmehr in Abs. § 36 Abs. 2 lit. a) klargestellt, dass Einrichtungen nach § 3 Abs. 1 lit b) und c) KDG einen betrieblichen Datenschutzbeauftragten bestellen müssen, wenn mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Insoweit entfallen die Diskussionen die um den Begriff „sollen“ stattgefunden haben, der in der KDO an dieser Stelle verwendet wurde.

Weder in der DSGVO noch im BDSG (neu) findet diese 10-Personengrenze eine Entsprechung. Eine nachvollziehbare Erklärung findet sich auch in der Begründung

zum KDG nicht. Wenn dort davon gesprochen wird, dass im kirchlichen Bereich oftmals kleinteiligere Strukturen zu finden sind, müsste dies gleichermaßen für Einrichtungen nach § 3 Abs. 1 lit a) KDG gelten. Damit die Regelung trotzdem im Einklang mit der DS-GVO steht (Art. 91 Abs. 1 DSGVO) steht, ist sie eng auszulegen.

Die Formulierung „ständig“ kann deshalb nicht im Sinne von „ausschließlich“ verstanden werden. Vielmehr ist darunter zu verstehen, dass der jeweilige Mitarbeiter für die sinnvolle Erfüllung seiner arbeitsrechtlichen Verpflichtungen auf eine IT-gestützte Verarbeitung personenbezogener Daten nicht verzichten kann. Dies schließt regelmäßig alle Mitarbeiter ein, die mit einem IT-Endgerät (APC, Laptop, Tablet u.ä.) arbeiten. Ausnahmen sind bestenfalls im Bereich von Haus- und Hofarbeitern, Fahrern u. ä. Mitarbeitern denkbar.

Für die Berechnung der Anzahl ist ferner unerheblich, in welchem Umfang oder auf welcher Rechtsgrundlage die Personen beschäftigt sind. Wie auch nach der KDO fallen also auch Ehrenamtliche, Praktikanten, Auszubildende, FSJ´ler, Mini- und „Ein-Euro- Jobber“ u.ä. darunter.

Auch die Einrichtungen nach § 3 Abs. 1 lit. b und c, in denen weniger als zehn Personen beschäftigt sind, haben einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn die Voraussetzungen des § 36 Abs. 2 lit. b und c erfüllt sind.

Unter Kerntätigkeiten sind solche Tätigkeiten zu verstehen, die erforderlich sind, um die Zielsetzung oder die Aufgabe der Einrichtung direkt zu erreichen.

Umfangreich ist eine Tätigkeit, nicht erst wenn sie in einer „über das übliche Maß“ hinausgehenden Weise verarbeitet werden[9], sondern bereits dann, wenn besondere Kategorien personenbezogener Daten in relevanter Weise, also nicht nur im Einzelfall, verarbeitet werden.[10] Damit fallen auch kleinere Einrichtungen z. B. der Ehe- Familien- Lebensberatung, oder der Schuldnerberatung unter die Bestellungspflicht.

3.2. Datenschutzkoordinator

Gem. § 36 Abs. 5 KDG steht es den Einrichtungen frei, einen Beschäftigten des Verantwortlichen zum betrieblichen Datenschutzbeauftragten zu ernennen oder die Aufgabe aufgrund eines Dienstleistungsertrages an einen Auftragsverarbeiter zu vergeben.

Einige Einrichtungen haben nunmehr einen dritten Weg gewählt. Dort wurde ein externer betrieblicher Datenschutzbeauftragter auf der Grundlage einer

[9] So Paal / Pauly DS-GVO Art 37 Rn. 9
[10] Helfrich in Sydow EU DS-GVO Art. 37 Rn. 92

Honorarvereinbarung bestellt. Gleichzeitig aber intern ein sogenannter „Datenschutzkoordinator“ berufen. Dessen Aufgabenbeschreibung dann u. a. folgende Formulierung enthält:

„Mitarbeiter sollen sich über den Datenschutzkoordinator an den externen Datenschutzbeauftragten wenden, damit dieser einen Überblick über die datenschutzrelevanten Themen des Unternehmens erhält.“

Weiter koordiniert und bündelt er Fragen zum Datenschutz sowie Anfragen Betroffener, die er/sie an den externen betrieblichen Datenschutzbeauftragten weiterleitet. Er kann wiederholende Fragen selbständig beantworten.“

Diese Regelung verstößt gegen § 37 Abs. 3 KDG. Durch die Vorgabe wird das Gesetz in unzulässiger Weise eingeschränkt.

Ziel dieser Regelung ist, was auch in der Aufgabenbeschreibung für den Datenschutzkoordinator dargestellt wird, eine Filterung der Anfragen der Betroffenen. So kann der nicht weisungsfreie Datenschutzkoordinator festlegen, welche Fragen er selber beantwortet und damit einer Kontrolle durch den betrieblichen Datenschutzbeauftragten vorenthält. Auf diese Weise lenkt der Verantwortliche die gemeldeten Datenschutzanfragen und kann eine gebotene Befassung des betrieblichen Datenschutzbeauftragten verhindern. Gem. § 38 Abs. 1 KDG hat der betriebliche Datenschutzbeauftragte das Recht und die Pflicht, sich in Zweifelsfällen an die Datenschutzaufsicht zu wenden. Dem Datenschutzkoordinator wird eine solche Rechtsstellung nicht eingeräumt.

Sollten die Verantwortlichen mit dieser „Rechtsfigur eigener Art“ die Absicht verfolgen, durch eine geringere, weil seltenere Inanspruchnahme des externen betrieblichen Datenschutzbeauftragten, Kosten zu sparen, ist dieser Ansatz unakzeptabel.

3.3. Betrieblicher Datenschutzbeauftragter

3.3.1. Erreichbarkeit

§ 36 Abs. 3 KDG lässt zu, für mehrere kirchliche Stellen unter Berücksichtigung ihrer Organisationsstruktur und Größe einen betrieblichen Datenschutzbeauftragten zu bestimmen. Diese Reglung entspricht der in Art. 37 Abs. 3 DSGVO. Darüber hinaus ist in der europäischen Regelung in Art. 37 Abs. 2 für Unternehmensgruppen die Möglichkeit festgestellt, einen gemeinsamen betrieblichen Datenschutzbeauftragten zu ernennen. Während im Fall des behördlichen Datenschutzbeauftragten nur Größe

und Organisationsstruktur der Behörde zu berücksichtigen ist, ist Voraussetzung für Unternehmen, dass der Datenschutzbeauftragte von jeder Niederlassung leicht erreichbar sein muss. Im KDG fehlt diese Differenzierung. Das KDG gesteht unter § 37 Abs. 3 jedem Betroffenen zu, sich jederzeit und unmittelbar an den betrieblichen Datenschutzbeauftragten wenden zu können.

Um diesen Anspruch erfüllen zu können, ist auch für das KDG „leichte Erreichbarkeit" des Datenschutzbeauftragten im Sinne einer persönlichen Erreichbarkeit[11] zu fordern. Das ergibt sich u. a. auch aus den Aufgabenzuweisungen des Art. 39 Abs. 1 lit. a) DSGVO. Die dort geforderte Beratung des Verantwortlichen, des Auftragsverarbeiters und der Beschäftigten macht regelmäßig ein persönliches Zusammentreffen erforderlich.[12] Das gleiche gilt im Hinblick auf die in Art. 38 Abs. 5 DSGVO festgeschriebene Wahrung der Gemeinhaltung und Vertraulichkeit des betrieblichen Datenschutzbeauftragten, auch diese Forderung macht eine persönliche Anwesenheit erforderlich.[13]

Auch wenn das KDG die „leichte Erreichbarkeit" nicht ausdrücklich fordert, ist das Recht auf jederzeitige und unmittelbare Kontaktaufnahme im selben Sinne zu verstehen. Um den betrieblichen Datenschutzbeauftragten unmittelbar persönlich kontaktieren zu können, muss der Betroffene oder der Verantwortliche diesen maximal innerhalb eines achtstündigen Arbeitstages erreichen können. Dies stellt eine maximalle Grenze dar, die Hin- und Rückfahrt inkludiert.[14]

Fraglich erscheint, ob das in den Bistümern, die für nahezu alle Pfarreien und Einrichtungen einen gemeinsamen Betrieblichen Datenschutzbeauftragten bestellt haben, zutrifft.

Insbesondere wenn drei Bistümer für nahezu alle Pfarreien und Einrichtungen ihres Bistumsgebietes einen einzigen externen Betrieblichen Datenschutzbeauftragten bestellt haben, stellt sich die Frage, der Belastbarkeit dieses Betrieblichen Datenschutzbeauftragten. Außerdem ist in diesem Fall zu klären, ob es noch weitere Kunden gibt, die dieser externe Betriebliche Datenschutzbeauftragte betreut, oder ob eine der Weisungsfreiheit entgegenstehende Abhängigkeit von den kirchlichen Auftraggebern besteht.

[11] Sydow DSGVO Art. 37 Rn. 96; Paaal/Pauly DSGVO Art. 37 Rn. 10; Heidelberger Kommentar Jasper/ Reif Art. 37 Rn. 32
[12] Heidelberger Kommentar Jasper/ Reif Art. 37 Rn. 32
[13] Sydow, Art. 37 Rn. 97
[14] So auch Heidelberger Kommentar Jaspers/Reif Art. 37 Rn., 32 für die europäische Gesetzesregelung

3.4. Haftung des betrieblichen Datenschutzbeauftragten

Zum betrieblichen Datenschutzbeauftragten kann ein Mitarbeiter bestellt werden (interner betrieblicher Datenschutzbeauftragter) oder ein Unternehmen, ein Anwalt o. ä. (externer Datenschutzbeauftragter). Nach den Vorschriften des KDG sind nunmehr auch die Pfarreien verpflichtet, betriebliche Datenschutzbeauftragte zu bestellen. Da insbesondere in den Pfarreien die Bestellung von Privatpersonen präferiert wird, kommen von diesen auch verstärkt Anfragen zur Haftung der betrieblichen Datenschutzbeauftragten, bzw. zur Möglichkeit einer entsprechenden Versicherung. Deshalb ist eine Darstellung der Haftung auch an dieser Stelle geboten.

3.4.1. Strafrechtliche Haftung

Eine solche scheidet regelmäßig für den betrieblichen Datenschutzbeauftragten aus.

Er ist weder Weisungs- noch Anordnungsbefugt. Eine Straftat kann somit nur durch die verantwortliche Stelle begangen werden, da allein diese die Verantwortung für die Einhaltung der Datenschutzgesetze trägt.

Ausnahme: Strafbarkeit nach § 203 StGB, wenn der bDSB ein fremdes Geheimnis offenbart, von welchem der bDSB bei seiner Berufsausübung erfahren hat.

In dieser Hinsicht spielt die Frage der internen oder externen Bestellung keine Rolle.

3.4.2. Zivilrechtliche Haftung

3.4.2.1. Ansprüche des Betroffenen

Da zwischen dem bDSB und der betroffenen Person kein Vertragsverhältnis besteht, scheiden vertragliche Schadensersatzansprüche gegen den bDSB und damit eine Haftung aus.

Grundsätzlich denkbar wären aber deliktische Ansprüche gegen den bDSB. Dies setzt aber voraus, dass die eingetretene Verletzung unmittelbar auf das Verhalten des bDSB zurückzuführen wäre. Angesichts seiner fehlenden direkten Einflussmöglichkeiten dürfte ein solcher Beweis regelmäßig schwerfallen.

3.4.2.2. Ansprüche der verantwortlichen Stelle

Ansprüche gegenüber dem internen bDSB

Eine Haftung kommt gem. §§ 280 ff. BGB in Betracht. Zu berücksichtigen ist aber die Haftungserleichterung im Arbeitsrecht gem. § 619a BGB. Der Arbeitgeber müsste dem Arbeitnehmer sein Verschulden beweisen.

Es gelten außerdem die von der Rechtsprechung entwickelten Haftungserleichterungen im Arbeitsrecht.

Ansprüche gegenüber dem externen bDSB

Die Haftung ergibt sich aus den Regelungen des Geschäftsbesorgungsvertrages. Eine dem § 619a BGB vergleichbare Regelung fehlt.

Auch Haftungserleichterungen sind in diesem Fall nicht vorgesehen.

Für beide Fälle gilt jedoch, dass eine Haftung des bDSB nur dann in Betracht kommt, wenn diesem von der verantwortlichen Stelle alle erforderlichen Informationen über die Datenverarbeitung gewährt worden sind.

Hier dürfte es bei der Bestellung externer bDSB häufig zu Problemen kommen, da diese aufgrund der Honorarverträge nur zeitweise in die Einrichtung geholt und mit einem punktuellen Problem konfrontiert werden. Hier liegt der Haftungsausschluss mangels zureichender Information auf der Hand.

4. Datenschutz im Arbeitsrecht

4.1. Compliance und Datenschutz im Arbeitsverhältnis

4.1.1. Einleitung

Der Begriff stammt ursprünglich aus dem amerikanischen und lässt sich mit „Befolgung“ oder „Einhaltung“ übersetzen.[15] Bereits diese Übersetzung lässt vermuten, dass es Inhalt von Compliance ist, die Einhaltung von Vorschriften auch zu überwachen. Hierbei ist darauf zu achten, dass die Maßnahmen zur Compliance ihrerseits selber rechtmäßig sein müssen und gesetzliche Vorschriften, zu denen auch der Datenschutz gehört, nicht verletzten dürfen. Compliance und Datenschutz haben richtig verstanden dieselbe Zielrichtung. Dennoch werden beide Begriffe häufig als gegensätzlich oder zumindest als einander störend empfunden.

[15] so auch Thüsing, Beschäftigtendatenschutz und ComlianceRn. 2

4.1.2. Begriff

Bislang gibt es weder eine gesetzliche Definition von Compliance, noch ist eine allgemein anerkannte Definition vorhanden.[16] So umfasst Compliance zum einen die Gesamtheit aller Maßnahmen, um das rechtmäßige Verhalten der Unternehmen, der Organmitglieder und der Arbeitnehmer im Blick auf alle gesetzlichen Gebote und Verbote zu gewährleisten.[17] Nach der Definition des Deutschen Corporate Governance Kodex soll Compliance sicherstellen, dass Unternehmen und deren Beschäftigte im Einklang mit geltenden Regeln und Gesetzen handeln.[18] Danach umfasst sind also nicht nur formale Gesetze sondern auch Verpflichtungen, die sich das Unternehmen selbst auferlegt, wie z. B. Ethik- und Umweltrichtlinien, die Präventionsrichtlinie oder Arbeitsanweisungen, Organisationshandbücher u.a.[19] Ein Compliance-System ist damit auch geeignet, die Reputation des Unternehmens in der Öffentlichkeit zu stärken.[20] So legt der Corporate Governance Kodex der Diakonie als Ziel fest, das Vertrauen der Menschen, für die diakonische Einrichtungen und Dienste da sind, sowie das Vertrauen der Öffentlichkeit, der Mitarbeitenden, der Politik und der Menschen, die die Diakonie mit ihren Spenden unterstützen, zu stärken.[21]

4.1.3. Compliance im Beschäftigtenkontext

Der Arbeitgeber hat ein Interesse daran, dass sich seine Beschäftigten gesetzes- und regelkonform verhalten. Dies betrifft neben der Wahrung seiner eigenen Vermögensinteressen auch die Außendarstellung des Unternehmens. Im Sinne der Definition von Compliance ist deshalb eine Überwachung auch der Mitarbeiter möglich. Dabei sind jedoch Regeln einzuhalten, damit die Persönlichkeitsrechte der Mitarbeiter gewahrt bleiben und ihr Vertrauen in die Einrichtung nicht gefährdet wird, da genau dies ebenfalls Inhalt von Compliance ist.

Compliance besteht in der Regel aus einem Bündel von Maßnahmen, welches sowohl präventive als auch repressive Vorgehensweisen umfassen kann. Dazu gehören u. a. Videoüberwachung, Kontrolle der E-Mail- und Internet-Nutzung, elektronische

[16] Vetter in Wecker/Ohl Compliance in der Unternehmerpraxis 2.1
[17] Lelley, Compliance im Arbeitsrecht S. 9; Schneider ZIP 2003,645;
[18] Deutscher Corporate Governance Kodex Nr. 4.1.3; Krieger/Günther, NZA 2010, 367; Bürkle BB 2005, 565,
[19] so auch Bürkle, BB 2005, 565, 569;
[20] Bergmoser/Theusinger/Gushorst, BB-Special zu Heft 5 2008, 1, 2;
[21] Diakonischer Corporate Governance Kodex 2016, S. 3

Datenabgleiche von Stammdaten der Beschäftigten mit Lieferantendaten oder Einrichtung von Whistleblower Hotline.[22]

Werden für Beschäftigungszwecke Daten verarbeitet, ist diese Verarbeitung an den Anforderungen der DSGVO und des BDSG[23] zu messen. Die grundsätzliche Weichenstellung für die Zulässigkeit der genannten Maßnahmen erfolgt durch § 26 BDSG[24].

Zu unterscheiden ist der allgemeine Rechtfertigungsgrund gem. § 26 Abs. 1 S. 1 BDSG[25] und der spezielle Rechtfertigungsgrund nach § 26 Abs. 1 S. 2 BDSG.[26]

§ 26 Abs. 1 S. 2 BDSG regelt die Verarbeitung personenbezogener Daten zur Aufdeckung von Straftaten, betrifft also repressive Maßnahmen. Eingriffe in die Grundrechte der Arbeitnehmer sind danach nur dann zulässig, wenn es einen konkreten Anhaltspunkt für einen Tatverdacht gibt.[27] Dieser durch Tatsachen begründete Verdacht einer strafbaren Handlung ist zu dokumentieren (§ 26 Abs. 1 S. 2 2. Hs).

Der Anwendungsbereich dieser Vorschrift ist somit auf die Aufdeckung von Straftaten im Beschäftigungsverhältnis beschränkt.[28] Der Verdacht begangener Ordnungswidrigkeiten rechtfertigt den Eingriff also nicht.[29] Außerdem müssen weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sein. Der Eingriff muss das praktisch einzig verbleibende Mittel darstellen und darf nicht unverhältnismäßig sein.[30]

Sollen Straftaten verhindert werden, handelt es sich um präventive Maßnahmen. Bei diesen werden alle Mitarbeiter gleichbehandelt. Ein Beispiel dafür ist das Screening (4.1.3.2.), dem die Stammdaten aller Mitarbeiter unterzogen werden um Korruption zu verhindern. Sobald man einzelne oder Gruppen herauslöst und nur diese

[22] Internetauftritt der BfDI Compliance und Datenschutz zuletzt eingesehen 09.07.2018
[23] Das Gesetz über den kirchlichen Datenschutz (KDG) gilt für Einrichtungen der katholischen Kirche gem. § 3 Abs. 1 KDG, Das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) gilt für evangelische Einrichtungen gem. § 2 Abs. 1 DSG-EKD.
[24] § 53 KDG, § § 49 DSG-EKD
[25] § 49 Abs. 1 DSG-EKD, § 53 Abs. 1 KDG. Die im KDG nicht enthaltene Ergänzung im BDSG § 26 Abs. 1 S. 1 a. E., mit der auf kollektivvertragliche Regelungen hingewiesen wird, stellt im BDSG lediglich eine Klarstellung der auch bislang geltenden Rechtslage dar, BT.-Drs. 18/11325, S. 97. Das Fehlen im KDG stellt mithin keine inhaltliche Differenz dar.
[26] § 53 Abs. 2 KDG, § 49 Abs. 2 DSG-EKD
[27] ArbG Cottbus, Urteil vom 25.11.2015 – 3 Ca 359/14; Thüsing Beschäftigtendatenschutz und Compliance, § 11 Rn. 46
[28] Seifert in Simitits Kommentar zum BDSG § 32. Rn. 102;Gola BB, 2017, 1466 mit Angabe von Beispielen
[29] Franzen in Erfurter Kommentar zum Arbeitsrecht, 17. Auflage 2017 § 32 BDSG Rn. 32; Seifert in Simitis § 32 Rn. 102
[30] BAG 21.11.2013 – 2 AZR 797/11 (juris Rn. 50)

beobachtet, handelt es sich um einen Verdacht gegenüber diesen Einzelnen oder der betreffenden Gruppe. [31]

Für präventive Maßnahmen gelten die geringeren Anforderungen des § 26 Abs. 1 S. 1. Ein konkreter Verdacht ist nicht erforderlich. Ausreichend ist vielmehr eine besondere Gefahrenlage, bzw. Gefährdung für die Interessen des Eigentümers. Ausreichend ist im ersten Prüfungsschritt eine abstrakte Gefahr, im zweiten Prüfungsschritt ist dann eine Verhältnismäßigkeitsprüfung erforderlich.[32] Führt der Arbeitgeber Überwachungsmaßnahmen oder Kontrollen zur Prävention durch, muss er dabei darauf achten sich selber compliant zu verhalten.[33] Einige Beispiele sollen dies verdeutlichen:

4.1.3.1.Videoüberwachung

Jede Videoüberwachung, gleich ob damit aufgezeichnet oder nur beobachtet wird, tangiert die freie Entfaltung der Persönlichkeit des Mitarbeiters und erzeugt einen mit der Wahrung dieser Persönlichkeitsrechte nicht zu vereinbarenden Überwachungsdruck.[34] Das gilt auch für die Fälle, in denen die Videoüberwachung zwar grundsätzlich bekannt ist, die Mitarbeiter jedoch nicht wissen, wann Aufzeichnungen stattfinden.[35] Eine präventive Videoüberwachung der Mitarbeiter scheidet, wenn sie heimlich stattfindet schon deshalb aus, weil sie keine abschreckende Wirkung entfalten kann.[36] Aber auch eine Dauerbeobachtung wegen der abstrakten Gefahr von Delikten ist nicht erforderlich. Solche Überwachungsmaßnahmen widersprechen einer Compliance, weil damit nicht Vertrauen geschaffen, sondern Misstrauen kultiviert wird.

Eingriffe in das Recht der Arbeitnehmer am eigenen Bild durch verdeckte Videoüberwachung sind dann zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist. [37]

[31]Thüsing NZA 2017 S. 1029
[32]Thüsing Compliance § 11 Rn. 35
[33] BAG 27.07.2017 – 2 AZR 573/06
[34] BAG NZA 1992, 43; BAG 1 ABR 16/07 Rn 15
[35]Gola, Datenschutz am Arbeitsplatz Rn. 78;
[36] Däubler, Gläserne Belegschaften Rn. 312b
[37] BAG 20.10.16 – 2 AZR 395/15; BAG 27. März 2003 – 2 AZR 51/02

4.1.3.2. Keylogger

Ein Keylogger ist eine Hard- oder Software, die dazu verwendet wird, sämtliche Eingaben des Benutzers an der Tastatur eines Computers zu protokollieren und damit zu überwachen oder zu rekonstruieren. Installiert der Arbeitgeber heimlich oder ohne Zustimmung des Arbeitnehmers einen Keylogger um damit dessen vertragskonformes Verhalten zu kontrollieren, stellt dies einen massiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung des Arbeitnehmers dar. Die Einrichtung einer solchen Technik ist unzulässig, durch eine solche Installation gewonnenen Erkenntnisse unterliegen in einem Kündigungsrechtsstreit einem Beweisverwertungsgebot.[38]

4.1.3.2. Screening

Compliance wurde ursprünglich zur Korruptionsverhinderung eingesetzt. Oftmals werden die Begriffe deshalb heute auch noch gleichgesetzt.[39] Zwar greift das, wie bereits dargelegt zu kurz, aber dennoch besteht eine wichtige Aufgabe von Compliance darin, Bestechung und Bestechlichkeit zu verhindern. Eine Möglichkeit besteht darin, mit Hilfe des sogenannten Screenings Stammdaten der Beschäftigten mit denen der Lieferanten oder Dienstleister abzugleichen.[40] Derartige Screenings werden in der Regel präventiv erfolgen und können unter bestimmten Voraussetzungen erlaubt sein. Der Abgleich hat zunächst mit pseudonymisierten Daten stattzufinden und darf erst im Verdachtsfall personalisiert werden.[41] Dabei wird es nicht gerechtfertigt sein, alle Beschäftigten mit einzubeziehen, sondern nur diejenigen, deren Daten für den zuvor festgelegten Zweck erforderlich sind. Auch ist der Abgleich transparent und nicht geheim durchzuführen. Mitarbeitervertretung und Datenschutzbeauftrage sind daran zu beteiligen.[42]

4.1.3.4. Whistleblowing-Hotline

Um die Einhaltung von Gesetzen und Regeln zu überwachen, bieten Unternehmen ihren Mitarbeitern und Kunden teilweise sogenannte Whistleblower Hotlines an, über die sie der Leitung außerhalb der regulären Informations- und Meldekanäle von Missständen berichten können.[43] Die Hotlines sind häufig anonym ausgestaltet. Grundsätzlich sind solche Maßnahmen zulässig. Es ist aber der Einzelfall zu

[38]LAG Hamm, Urteil vom 17.06.2016 - 16 Sa 1711/15; CR 2017, 99; BAG Urteil vom 27.7.2017, 2 AZR 681/16
[39] Internetauftritt der BfDI Compliance und Datenschutz zuletzt eingesehen am 09.07.2018
[40]Gola/Pötters/WronkaRn. 1340
[41]Gola Datenschutz am Arbeitsplatz Rn. 209
[42]Wybitull BB 2009, 1582
[43] Orientierungshilfe der Datenschutzaufsichtsbehörden vom 17.01.2018 S. 3

beurteilen. Wenn sich das Whistleblowern auf harte Verstöße, wie gegen das Unternehmen gerichtete Straftatbestände oder auf Verhaltensweisen, die gegen Menschenrechte gerichtet sind fokussiert, wird man von einer Zulässigkeit ausgehen müssen. Bei weichen Verstößen, wie internen Anweisungen zum Umgang mit Kunden, dürften solche Maßnahmen unzulässig sein.

4.1.4. Verhältnis des betrieblichen Datenschutzbeauftragten zum Compliance-Officer

Die Bestellung eines betrieblichen Datenschutzbeauftragten ist in Art 37 DSGVO [44] gesetzlich vorgesehen. Der Compliance-Officer hat also auf dessen Bestellung hinzuwirken, damit der Verantwortliche diesbezüglich seine gesetzliche Pflicht erfüllt.

Der betriebliche Datenschutzbeauftragte berät die Geschäftsführung in Fragen des Datenschutzes. Er hat darauf hinzuweisen, welche Vorschriften einzuhalten oder welche Maßnahmen umzusetzen sind. Er ist für deren Überwachung zuständig, aber nicht verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben, da er keine Entscheidungs- oder Weisungsbefugnisse besitzt.[45]

Anderes gilt für den Compliance Officer, dessen Aufgabengebiet die Verhinderung von Rechtsverstößen ist, die aus dem Unternehmen heraus begangen werden und diesem erhebliche Nachteile durch Haftungsrisiken oder Ansehensverlust bringen können. Derartig Beauftragte wird regelmäßig strafrechtlich eine Garantenpflicht im Sinne des § 13 Abs. 1 StGB treffen, solche im Zusammenhang mit der Tätigkeit des Unternehmens stehende Straftaten von Unternehmensangehörigen zu verhindern.[46] Eine solche Überwachergarantenstellung trifft aber eben nicht den betrieblichen Datenschutzbeauftragten.[47]

4.1.5. Zusammenfassung

Die Einführung von Compliance Richtlinien ist sinnvoll und zeitgemäß, insbesondere wegen der Erkenntnis, dass das Unternehmen nicht nur die gesetzlichen Vorgaben zu erfüllen hat, sondern auch für eine Einhaltung darüberhinausgehender Regeln zu sorgen hat. Wird die Befolgung von Regeln nicht überwacht, verkommen diese zu bloßen Programmsätzen. Dies rechtfertigt aber nicht eine permanente und anlasslose

[44] § 36 KDG, § 36 DSG-EKD
[45] Jaspers/Reif Heidelberger Kommentar DS-GVO/BDSG Art. 39 Rn.14
[46] BGH Urteil vom 17.07.2009 – 5 StR 394/08
[47] Landwin ZD 2017, 411, 414

Kontrolle der Mitarbeiter. Bei der praktischen Umsetzung von Compliance Regeln ist deren Sinn und Zweck zu beachten, der vor allem auch in der Schaffung von Vertrauen bei den Mitarbeitenden besteht und so Auswirkungen auf die Reputation des Unternehmens hat.

4.2. Darf der Arbeitgeber E-Mails lesen

4.2.1. Einführung

Fast jeder Arbeitsplatz ist heute mit einem Arbeitsplatzcomputer (APC) ausgestattet. Dieser verfügt regelmäßig über einen Internetzugang und ist geeignet und dafür vorgesehen, E-Mails zu erhalten und zu versenden. Während sich arbeitsrechtlich die Frage stellt, ob der Mitarbeiter diese Technik privat nutzen darf, stellt sich datenschutzrechtlich die Frage, ob der Arbeitgeber Einblick in das Nutzungsverhalten und die Kommunikation der Mitarbeiter nehmen darf. Hier sind zunächst drei Grundkonstellationen zu unterscheiden: I. Der Arbeitgeber hat die private Nutzung verboten[48]. II. Der Arbeitgeber hat die Nutzung, evtl. unter Auflagen erlaubt. III. Der Arbeitgeber hat beides nicht getan und duldet die private Nutzung oder er hat zwar ein Verbot ausgesprochen, kontrolliert die Einhaltung aber nicht oder duldet wissentlich Zuwiderhandlungen.

4.2.2. Der Arbeitgeber hat die private Nutzung untersagt

Der Arbeitgeber stellt dem Arbeitnehmer Betriebsmittel und technische Geräte zur Verfügung, damit dieser seine arbeitsvertraglich geschuldete Tätigkeit verrichten kann. Eine darüberhinausgehende private Nutzung dieser Einrichtungen bedarf der vorherigen Genehmigung des Arbeitgebers. Eine nicht genehmigte Privatnutzung während der Arbeitszeit ist grundsätzlich unzulässig und stellt eine Verletzung der arbeitsvertraglichen Hauptpflicht dar, die der Arbeitgeber abmahnen darf.[49] Abhängig von der Schwere des Verstoßes ist auch eine verhaltensbedingte Kündigung möglich.[50]

[48] BAG Urteil vom 7.7.2005 – 2 AZR 581/04; NZA 2006, 98
[49] BAG Urteil vom 19.04.1012, 2 AZR 186/11
[50] LAG Hessen, Urteil vom 13.12.2001, 5 Sa 987/01; LAG Niedersachsen 31.05.2010, 12 Sa 875/09

Eine Internet- / E-Mail- Nutzung ist dann dienstlich, wenn ein spezifischer Bezug zu den Arbeitsaufgaben des Arbeitnehmers besteht.[51] Der Arbeitnehmer muss bei der Nutzung also die Absicht haben, damit seine Arbeitsaufgabe zu erfüllen.

Eine Ausnahme stellen private E-Mails dar, die dienstlich veranlasst sind (z. B. Mitteilung an den Partner, dass man am Abend wegen eines dienstlichen Besprechungstermins später nach Hause kommt). Diese sind ebenso wie dienstlich veranlasste Privattelefonate auch bei verbotener Privatnutzung zulässig.

E-Mails sind Geschäftsbriefe, die der jederzeitigen Überprüfbarkeit durch den Arbeitgeber unterliegen.[52] Fraglich ist, ob dies auch dann gilt, wenn die Mitteilung an einen persönlichen Account des Mitarbeiters gesendet wird (z. B. Max Mustermann@xGmbH). Nach einer Ansicht in der Literatur darf der Absender auch in diesem Fall nicht darauf vertrauen, dass die Mitteilung nur vom Empfänger gelesen wird.[53] Zu berücksichtigen ist jedoch, dass bei einem persönlichen Account der Absender anders als bei der Namensnennung im Anschriftenfeld eines Briefes davon ausgehen kann, dass die Mitteilung den Empfänger direkt erreicht. Bei einem Brief dient die Namensangabe hingegen regelmäßig nur der Zuordnung der Mitteilung zu einem bestimmten Bearbeiter, die Post wird jedoch üblicherweise in der Poststelle geöffnet.[54] Da durch den persönlichen Account dem Absender nahegelegt wird, dass seine Mitteilung direkt beim Empfänger auf dessen Arbeitsplatzcomputer eingeht und nur dieser Kenntnis davon nimmt, darf der Absender insoweit von einer bestehenden Vertraulichkeit ausgehen. In diesem Fall steht die E-Mail Korrespondenz dem Telefonat näher als der Briefpost.[55] Deshalb ist auch bei einer ausschließlich dienstlich erlaubten Nutzung eine Interessenabwägung erforderlich. Nur wenn überwiegende Arbeitgeberbelange dafürsprechen, ist bei der Verwendung persönlicher E-Mail Accounts ein Einsichtsrecht des Arbeitgebers gegeben.[56]

Befinden sich in einem ausschließlich zur dienstlichen Nutzung überlassenen Mail-Account eines Arbeitnehmers private E-Mails, ist die Einsichtnahme durch den Arbeitgeber in die privaten E-Mails verboten.[57] Sobald der Arbeitgeber den privaten Inhalt erkennt, ist ein Weiterlesen oder ein andere Verwendung dieser Inhalte untersagt. Ebenso ausgeschlossen ist die inhaltliche Kenntnisnahme des Inhaltes von

[51] Kramer NZA 2004, 458; Becker in Kittner/Zwanziger Arbeitsrecht Handbuch für die Praxis § 72 Rn. 79a
[52] Linck in Schaub Arbeitsrechtshandbuch § 53 Rn. 18
[53] Gola, Datenschutz am Arbeitsplatz Rn. 384; Besgen/Prinz/Schumacher Handbuch Internet Arbeitsrecht §1 Rn.41
[54] Ernst NZA 2002 S. 589
[55] Däubler Gläserne Belegschaften? Rn. 351
[56] So wohl auch Seifert in Simitis Kommentar zum BDSG (alt) § 32 Rn. 92
[57] Orientierungshilfe der Datenschutzaufsichtsbehörden B. II. 3. (S.6)

E-Mails an die Interessenvertretung der Mitarbeiter (MAV, Jugend- u. Auszubildendenvertretung, Schwerbehindertenvertretung und Betriebsrat).[58]

4.2.3. Die private Nutzung von Internet und E-Mail-Account ist ausdrücklich erlaubt

Da die Kosten für den Arbeitgeber für Internet- und E-Mail Nutzung nicht zuletzt wegen häufig vereinbarter Flatrates zu vernachlässigen sind, wird Arbeitnehmern die private Nutzung dieser Medien häufig gestattet. Eine solche private Nutzung des Internets kann individuell mit dem Arbeitnehmer oder in einer Betriebsvereinbarung vereinbart sein, ebenso kann sie durch Aushänge oder "E-Mail an alle" vom Arbeitgeber erlaubt werden. Auch in diesem Fall ist aber zu beachten, dass eine ohne Auflagen bzw. nähere Konkretisierung bestehende Erlaubnis nicht zur grenzenlosen oder gar exzessiven Nutzung berechtigt.[59] Die Nutzung muss zeitlich und inhaltlich angemessen sein, darf keine unzumutbaren zusätzlichen Kosten erzeugen und keine Gefahren für das Betriebssystem mit sich bringen.[60]

Ist die private Nutzung des Internets und der des dienstlichen E-Mail Accounts erlaubt, ist nach Ansicht der Datenschutzaufsichten und des überwiegenden Teils der Literatur der Arbeitgeber als Dienstanbieter i.S.v. § 3 Nr. 6 TKG zu betrachten.[61] Die Rechtsprechung sieht teilweise den Arbeitgeber nicht als Dienstanbieter i.S.d. TKG an.[62] Eine höchstrichterliche Entscheidung steht derzeit noch aus.

Folgt man der Rechtsauffassung der Datenschutzaufsichtsbehörden, ist bei Erlaubnis der privaten Nutzung des E-Mail Accounts dem Arbeitgeber verwehrt, Kenntnis vom Inhalt der E-Mails zu nehmen. Dies betrifft alle E-Mails, da das Kontrollverbot für die privaten E-Mails auf die dienstlichen E-Mails durchschlägt[63]. Wenn sich bei einer gemischt dienstlichen und privaten Nutzung, dienstliche Daten nicht von privaten trennen lassen, so unterliegen alle dem besonderen Schutz. Jegliche Kontrolle von E-Mails ist dann im Grundsatz verboten.[64] Bei einem Verstoß setzt sich der Arbeitgeber der Strafbarkeit nach § 206 StGB aus.

[58] Seifert in Simitis § 32 BDSG-alt RN 91
[59] Linck in Schaub Arbeitsrechtshandbuch 17. Auflage § 53 Rn. 17; BAG Urteil vom 7.7.2005, BAG, Urteil vom 07.07.2005, 2 AZR 581/04
[60] Kramer, NZA 2004, 459; Kittner/Zwanziger Arbeitsrecht Handbuch für die Praxis § 72 Rn. 80
[61] „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und Internetdiensten am Arbeitsplatz". So auch Linck in Schaub Arbeitsrechtshandbuch § 53 Rn. 19, Kreitner in Küttner Personalhandbuch
[62] LAG Berlin Brandenburg, 14.1.16 – 5 Sa 657/15; Hessischer VGH, 19.5.2009, 6 A 2672/08;
[63] Mengel NZA 2017, 1496, Seifert in Simitis Kommentar zum BDSG (alt) § 32 Rn. 92
[64] Gola/Pötters/Wronka Handbuch Arbeitnehmerdatenschutz Rn. 1282

Hier entstehen vor allem dann Probleme, wenn der Arbeitnehmer so kurzfristig ausfällt (wegen Krankheit oder Unfall), dass ein Abwesenheitsagent von ihm nicht aktiviert werden kann und keine Zugriffsregelung für einen solchen Fall getroffen worden ist. Ohne Einwilligung des Arbeitnehmers ist dem Arbeitgeber in einem solchen Fall der Zugriff auf alle E-Mails grundsätzlich versperrt.

4.2.4. Stillschweigende Duldung der privaten Nutzung

Das gleiche gilt auch im Falle der stillschweigenden Duldung durch den Arbeitgeber. Hat dieser die private Nutzung zwar nicht ausdrücklich erlaubt, aber hingenommen, wird regelmäßig eine Betriebliche Übung entstanden sein. Diese liegt nicht schon dann vor, wenn in der Vergangenheit die private Nutzung ohne Beanstandung des Arbeitgebers stattgefunden hat.[65] Erforderlich ist vielmehr eine bewusste Duldung.[66] Der Arbeitnehmer muss also im Zweifel beweisen, dass der Arbeitgeber die private Nutzung in der Vergangenheit zur Kenntnis genommen hat, ohne über einen längeren Zeitraum dagegen einzuschreiten.[67]

Hinsichtlich der Frage, wann ein Zeitraum ein „längerer“ ist, fehlt eine abschließende Regelung. Eine Frist von einem Jahr[68] erscheint dabei zu lang. Spätestens nach einem halben Jahr darf der Arbeitnehmer darauf vertrauen, dass ihm diese Vergünstigung auf Dauer gewährt wird.

4.2.5. Widerruf der erlaubten Nutzung

Wenn der Arbeitgeber die private Nutzung in Zukunft untersagen will, ist die Zulässigkeit einer Rücknahme davon abhängig, ob die Gestattung zu den arbeitsvertraglichen Arbeitsbedingungen gehört oder der Arbeitgeber sich den Widerruf vorbehalten hat.

Ist letzteres nicht der Fall, so kann der Widerruf der Erlaubnis grundsätzlich nur im Wege der Änderungskündigung erfolgen.

[65] Beckschulze DB 2007, 1526
[66] LAG Hessen 25.07.2011, 17 Sa 1818/10
[67] Gola/Pötters/Wronka Handbuch Arbeitnehmerdatenschutz Rn. 1275 mit Hinweis auf Ernst NZA 2002, 585 der einen längeren Zeitraum bei einem halben Jahr als gegeben ansieht, während Kramer NZA 2004, 457 ein Jahr ansetzt.
[68] Kramer, Internetnutzung als Kündigungsgrund NZA 2004, 257f.

4.2.6. Empfehlung für die Praxis

1. Es sollte unbedingt eine Trennung von dienstlichen und privaten E-Mail-Adressen stattfinden, ebenso wie eine separate Nutzung des Internet für private Zwecke. Häufig wird es aus den o. g. Gründen nicht möglich sein, den Mitarbeitenden die private Nutzung von Internet und E-Mail zu untersagen. Deshalb sollten hier zwischen den Betriebsparteien Dienstvereinbarungen vereinbart werden. Dabei bieten sich folgende Möglichkeiten an:

1.1. Es werden Gruppen-E-Mail-Adressen, z. B. *Buchhaltung@Einrichtung.de* eingerichtet. Auf diese können alle Mitarbeiter der jeweiligen Gruppe (z.B. Buchhaltung) zugreifen. Ein Vertretungsproblem bei Abwesenheit einzelner besteht dann nicht mehr, weil die Gruppe der Mitarbeitenden ohnehin das Zugriffsrecht auf diese Mails hat. Dabei wird für den Absender auch deutlich, dass nicht nur eine bestimmte Person Zugriff auf die Mail hat und er auf eine Vertraulichkeit insoweit nicht vertrauen kann.
Auf diesem Weg umgeht man auch ein zusätzliches Datenschutzproblem, nämlich die Bekanntgabe des Namens von Mitarbeitenden. Namen sind personenbezogene Daten. Diese dürfen ohne Einwilligung nur verarbeitet, also auch bekannt gegeben werden, wenn dies erforderlich ist. In der Regel also nur dann, wenn die Funktion des Mitarbeitenden das erfordert. Dies wird bei Mitarbeitenden die ein Amt mit Außenwirkung oder eine Leitungsfunktion wahrnehmen gegeben sein, nicht jedoch bei solchen der inneren Verwaltung.

1.2. Die Rechte der Mitarbeitenden können durch Bereitstellung eines „stand alone"-Rechners[69] für die private Nutzung oder durch die Einrichtung eines separaten W-LAN-Netzes, auf das die Mitarbeitenden mit privaten Endgeräten (Smartphone, Tablet, Notebook o.ä.) zugreifen können, gewahrt werden.

2. Kommt es zu einer plötzlichen Verhinderung des Mitarbeitenden, derentwegen ein Abwesenheitsagent durch ihn nicht aktiviert werden kann, ist ein solcher durch den Administrator zu installieren. Eingehende E-Mails sind dadurch zurück zu senden, mit dem Hinweis, wer der Vertreter ist. Der Absender kann dann entscheiden, ob er seine Nachricht an den benannten Vertreter senden möchte. Geschieht dieser Vorgang

[69] Ein Rechner, der nicht in das Serversystem der Einrichtung integriert ist

zeitnah, ist die Einsichtnahme in die E-Mails des verhinderten Mitarbeitenden nicht erforderlich.

3. Nach dem Ausscheiden eines Mitarbeitenden sollte die E-Mail-Adresse unverzüglich gelöscht werden, so dass keine weiteren E-Mails auf dieser Adresse mehr eingehen.

Mit dem Mitarbeitenden sollte bei dessen Ausscheiden eine Vereinbarung getroffen werden, um sicher zu stellen, dass seine Rechte gewahrt sind. Dazu kann beispielsweise der folgende Text verwendet werden: „Ich bestätige, dass ich alle privaten Dateien, die ich auf dienstlichen Endgeräten gespeichert/verarbeitet habe, dort gelöscht habe. Sollten sich dennoch private Dateien auf den Rechnern/Servern der Dienststelle/Einrichtung befinden, erkläre ich meine Zustimmung dazu, dass diese ohne eine vorherige Mitteilung an mich von der Dienststelle/Einrichtung gelöscht werden können."

4.3. Personenbezogen Daten in der Dienstkleidung

Ein Krankenhaus lässt die Dienstkleidung der Mitarbeiter durch eine externe Wäscherei reinigen. In der Dienstkleidung ist jeweils ein Chip integriert. Beim Auslesen dieses Chips kann festgestellt werden, welcher Abteilung das Kleidungsstück zuzuordnen ist, damit es nach der Reinigung auf die entsprechende Station zugestellt werden kann. Um ihren Service zu verbessern fordert die Wäscherei nunmehr das Krankenhaus auf, neben der Chip-Nr. weitere Daten auf dem Chip zu speichern, nämlich Personalnummer, Name, Abteilung, Kostenstelle, Eintritt, Austritt der Person, der diese Bekleidung zugeordnet ist.

Die Personalchefin bzw. die betriebliche Datenschutzbeauftragte wendeten sich an unsere Dienststelle um zu erfragen, ob eine Weitergabe von personenbezogenen Daten in diesem Umfang zulässig sei.

Bei den zusätzlich verlangten Angaben handelt es sich unstreitig um personenbezogene Daten. Die Erfassung dieser Daten auf einem Chip, der in die Kleidung integriert ist und von der Wäscherei ausgelesen werden kann, stellt eine Verarbeitung gem. § 4 Nr. 2 KDG dar. Für die Rechtmäßigkeit dieser Verarbeitung müsste eine der in § 6 Abs. 1 KDG genannte Begründungen vorliegen. Eine solche Begründung aber ist nicht ersichtlich. Allein die von der Wäscherei genannte Verbesserung des Services trägt eine solche Verarbeitung nicht. Insbesondere ist

auch nicht zu erkennen, welcher Zweck mit den weiteren Daten, die neben dem Namen abverlangt werden verfolgt werden soll, oder wie der Service dadurch verbessert werden soll.

Wenn es ein Problem bereitet, die bislang nur auf die entsprechende Station gelieferte Dienstkleidung entsprechenden Mitarbeitern zuzuordnen, kann dies durch Hinzufügen einer Nummer oder eines Pseudonyms geändert werden. Weiter Daten dürfen in diesem Zusammenhang nicht verarbeitet werden.

4.4. Regelmäßige Abforderung einer Lesebestätigung durch Vorgesetzte unzulässig

Es wird häufig als nachteilig bzw. belastend empfunden, wenn Absendende einer E-Mail regelmäßig eine Lesebestätigung verlangen. Beim Empfänger erweckt dies den Eindruck der Absender misstraue ihm und gehe davon aus, dass die Mail ohne Lesebestätigung nicht oder nicht schnell genug bearbeitet würde. Dies wird sich zum einen negativ auf das Betriebsklima auswirken, ist zum anderen aber ggf. rechtlich unzulässig.

4.4.1. Beweiswert der Lesebestätigung

Zunächst lässt sich mit einer Lesebestätigung nicht beweisen, dass der Empfänger den Text inhaltlich zur Kenntnis genommen hat. Eine Lesebestätigung gibt bestenfalls darüber Auskunft, dass die Mail geöffnet worden ist. Das muss aber nicht unbedingt der Empfänger getan haben, sondern kann vom Vertreter vorgenommen worden sein. Auch ist der Nachweis der Öffnung kein Beleg für das Lesen der Mail. Vielmehr kann die Mail vor der inhaltlichen Kenntnisnahme wieder geschlossen worden sein.

4.4.2. Zugangsbeweis einer E-Mail

In der Rechtsprechung scheinbar umstritten ist die Frage, ob es für den Beweis des Zugangs einer E-Mail einer Lesebestätigung bedarf[70]. Da zumindest das LAG Brandenburg die Begriffe Eingangs- und Lesebestätigung gleichbedeutend

[70] so LAG Berlin-Brandenburg Beschluss vom 27.11.2011, Az.: 15 Ta 2066/12, BGH, Beschluss vom 17.07.2013, Az. I ZR 64/13; a. A. OLG Düsseldorf, Beschluss vom 4.10.2002das ein Sendeprotokoll, welches die korrekte Adresseingabe enthält ausreichen lässt.

verwendet, lässt sich vermuten, dass die Unterschiede zwischen beiden Möglichkeiten dem Gericht nicht vertraut sind.

Eine E-Mail geht zu, wenn sie in die Mailbox des Empfängers oder der des Providers abrufbar gespeichert wird[71]. War eine Übermittlungsbestätigung durch den Absender angefordert worden, sendet der Mailserver des Empfängers automatisch, sobald die E-Mail im Postfach abgelegt wurde, eine Eingangsbestätigung. Wurde eine Lesebestätigung gefordert, kann diese erst erfolgen, wenn der Empfänger seine E-Mail geöffnet hat. Es steht ihm dann frei, die Lesebestätigung zu erteilen, oder dies zu unterlassen. Wenn eine Lesebestätigung gegeben wird, mag das den Zugang der E-Mail beweisen, aber aus einer nicht gegebenen Lesebestätigung ist nicht darauf zu schließen, dass die E-Mail nicht zugegangen ist.

Hieraus wird ersichtlich, dass es für den Nachweis des Zugangs auf jeden Fall nicht der Lesebestätigung bedarf. Diesen Zweck erreicht die Übermittlungsbestätigung. (In den gängigen Programmen, z. B. Microsoft Outlook, stehen beide Möglichkeiten zur Verfügung.)

Durch die Abforderung einer Lesebestätigung wird jedoch der oben erwähnte Druck auf den Empfänger ausgeübt, zu belegen, dass er bei ihm eingehende E-Mails zeitnah zur Kenntnis nimmt.

4.4.3. Arbeitnehmerkontrolle durch Lesebestätigung

Tatsächlich ist auf dem Weg der regelmäßigen Verwendung einer Lesebestätigung durch Vorgesetzte aber die permanente und anlasslose Kontrolle eines Arbeitnehmers möglich.

Eine solche Überwachung von Mitarbeitern verstößt nach ständiger Rechtsprechung gegen datenschutzrechtliche Grundsätze. Denn die Gewinnung von Daten des Beschäftigten ist nach dem Datenschutzgesetz (§53 Abs. 2 KDG) nur dann erlaubt, wenn der Arbeitgeber sich auf Tatsachen stützen kann, die den Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung begründen.[72]

Nach § 53 Abs. 1 KDG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses dann verarbeitet werden, wenn dies für dessen Durchführung oder Beendigung erforderlich ist. Dabei gehört zur Durchführung auch die Kontrolle, ob der Arbeitnehmer seinen Pflichten

[71] Palandt § 130 Rn. 7a
[72] BAG Urteil vom 27. Juli 2017 - 2 AZR 681/16

nachkommt.[73]Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (§ 4 Nr. 1 KDG).

Voraussetzung für eine solche Überwachung ist aber deren Erforderlichkeit. Diese besteht dann, wenn der Zweck der Maßnahme auf anderem Wege nicht erreicht werden kann. Wie bereits dargelegt, kann der Zugang einer E-Mail durch eine Übermittlungsbestätigung erfolgen. Die Kontrolle der inhaltlichen Kenntnisnahme ist durch eine direkte Ansprache des Mitarbeiters möglich. Eine solche Ansprache ist weit weniger geeignet, einen permanenten Überwachungsdruck beim Mitarbeiter zu erzeugen und greift nicht in gleicher Weise wie die automatische Überwachung in das Persönlichkeitsrecht des Mitarbeiters ein.

4.4.4. Ergebnis

Aus datenschutzrechtlicher Sicht ist die Nutzung der Sendeoption „Lesebestätigung“ nur in begründeten Ausnahmefällen zu verwenden. Eine regelmäßige Einstellung dieser Option ist zumindest im Über-Unterordnungsverhältnis zwischen Arbeitgeber und Arbeitnehmer unzulässig.[74]

4.5. Passwörter Weitergabe

Art. 32 DSGVO (§26 KDG, § 27 DSG-EKD) verlangen vom Verantwortlichen angemessene technische und organisatorische Maßnahmen zu implementieren, um Datensicherheit im Sinne eines angemessenen Schutzniveaus herzustellen.[75]

Nach dem Wortlaut der gesetzlichen Regelung ist in Abs. 1 Satz 2 lit) a als eine angemessene Maßnahme u. a. die Verschlüsselung benannt. Eine grundlegende Verschlüsselung findet durch eine Sicherung des Rechners und der darin befindlichen Dateien mit einem jeweiligen Passwort statt.

Ein solches Passwort soll einen Schutz im Sinne der Zugriffssicherheit gewähren und deshalb nur einer Person Zugriff auf die personenbezogenen Daten gewähren.

Technisch organisatorische Maßnahmen haben für die Zugriffssicherheit, Anwendungen, insbesondere Eingabe, Änderung und Löschung von Daten, zu protokollieren. Dabei ist in erster Linie zu protokollieren, wer, wann auf welche Daten zugegriffen hat. Der Datenbestand wird jeweils nur den Mitarbeitern zugänglich

[73] ebd.
[74] 34. Tätigkeitsbericht 2012 des Bremer Landesbeauftragten für Datenschutz
[75]Mantz in Sydow Kommentar zur DSGVO Art. 32 Rn. 6

gemacht, die damit arbeiten müssen. Aus diesem Grund ist das Passwort individuell festzulegen und nur vom Inhaber des Passworts zu verwenden.

Nach den gängigen Sicherheitsanforderungen[76] muss das **Passwort** aus **mindestens acht Zeichen** bestehen wobei darauf zu achten ist, dass Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen verwendet werden.

Das Passwort darf nicht an Dritte weitregegeben werden, um diesen einen Zugriff zu ermöglichen.

Unter der Bezeichnung „Dritte“ ist jede andere Person zu verstehen. Es ist in keinem Fall erforderlich, einen solchen Zugriff unter einem fremden Passwort zu ermöglichen. Die in der Praxis gelegentlich herrschende Ansicht, die Vorgesetzte müsse die Möglichkeit haben auf die Dateien ihrer Mitarbeiterin Zugriff zu haben, kann kein Argument dafür sein, dass Passwort an den Vorgesetzten herauszugeben. Auch dann nicht, wenn dieses in einem verschlossenen Umschlag in einem Tresor gelagert und nur im „Notfall“ geöffnet werden soll.[77] Es spricht grundsätzlich nichts dagegen, der Vorgesetzten den gleichen Zugriff auf dienstliche Daten einzuräumen wie dem Mitarbeiter. Dieser Zugriff hat aber unter dem Passwort der Vorgesetzten zu erfolgen.

Es besteht keine Verpflichtung des Mitarbeiters, Vorgesetzen das von ihm verwendete Passwort bekannt zu geben. Die gegenteilige Aufforderung durch Vorgesetzte an den Mitarbeiter stellt einen Datenschutzverstoß dar. Sollte der Vorgesetzte den Mitarbeiter gegen seinen Willen mit der Androhung von Sanktionen unter Druck setzen, kommt auch eine strafrechtliche Verfolgung dieses Vorgehens in Betracht.

Verlangt der Arbeitgeber die Bekanntgabe des Passwortes für den Zugang zu den E-Maildaten des Mitarbeiters, liegt hierin gegebenenfalls auch ein Verstoß gegen das Telekommunikationsgesetz

Ist die private E-Mail-Nutzung erlaubt oder gilt sie als erlaubt, weil sie vom Arbeitgeber trotz Kenntnis der privaten Nutzung nicht verboten wurde, ist der Arbeitgeber gegenüber den Beschäftigten und ihren Kommunikationspartnern zur Einhaltung des Fernmeldegeheimnisses verpflichtet. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist dem Arbeitgeber grundsätzlich nur mit

[76] www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html
[77] Dieses Vorgehen wurde widerholt bei Prüfungen vorgefunden.

Einwilligung der betreffenden Beschäftigten erlaubt.[78] Auch hier hat ein Verstoß unter Umständen strafrechtliche Konsequenzen.[79]

4.6. Private Handynummer für den Dienstgeber

Arbeitnehmer können nach zwei Urteilen des Thüringer LAG die Weitergabe ihrer privaten Mobilfunknummer an den Arbeitgeber verweigern.[80]

Ein Krankenhaus verlangte von seinen Angestellten neben der privaten Festnetznummer auch die Bekanntgabe der Handynummer, um diese im Notfall auch außerhalb des Bereitschaftsdienstes mobil erreichen zu können. Hintergrund war eine Systemänderung der Rufbereitschaft zur Einrichtung eines Notdienstes. Die Mitarbeiter sollten an Werktagen von den Rettungskräften per Zufallsprinzip angerufen werden können. Hiergegen wehrten sie sich. Einen vergleichbaren Fall hatte das Thüringer LAG zu entscheiden. Dieses gab den klagenden Angestellten in zweiter Instanz Recht und wies die Berufung des Arbeitgebers zurück.

Offenbleiben kann, ob überhaupt eine Anspruchsgrundlage für das Auskunftsverlangen besteht.

Die Verpflichtung zur Herausgabe der mobilen Telefonnummer stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Dieser müsste durch ein berechtigtes Interesse des Arbeitgebers gerechtfertigt sein. Eine Abwägung müsste dann zu dem Ergebnis kommen, dass der Eingriff angemessen ist.

Das ist hier aber zu verneinen, denn den Beschäftigten droht ständige Erreichbarkeit, ohne sich dem entziehen zu können. Diese Drucksituation würde fortlaufend bestehen. Deshalb kommt es nicht auf das Argument des Gesundheitsamts an, dass die Wahrscheinlichkeit für eine Kontaktaufnahme im Notfall eher gering ist. Zudem hat der Arbeitgeber durch eine Systemänderung der Rufbereitschaft selbst für die Situation gesorgt. Er hätte andere Möglichkeiten, Notfälle – wie in der Vergangenheit – abzusichern.

Die Revision wurde nicht zugelassen, denn die grundlegende Rechtslage ist geklärt. Der Eingriff in das Recht auf informationelle Selbstbestimmung muss durch ein entgegenstehendes, überwiegendes berechtigtes Interesse gerechtfertigt sein.

[78] Datenschutzkonferenz www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/02/OH_E-Mail_Internet_Arbeitsplatz.pdf
[79] Siehe § 206 Abs. 4 StGB
[80] LAG Thüringen vom 16.5.2018 (6 Sa 442/17 und 6 Sa 444/17)

4.7. Elektronische Personalakte

In einer Einrichtung ist geplant, elektronische Personalakten einzuführen. In diesem Zusammenhang wurde die Frage gestellt, wer auf die elektronischen Personalakten Zugriff nehmen darf.

Diese Frage stellt sich zunächst gleichermaßen für elektronische, wie für analog geführte Personalakten. In diesen Akten sind personenbezogene Daten i. S. v. § 4 Nr. 1 KDG gespeichert (Name, Geburtsname, Geburtstag Adresse u.a.). Darüber hinaus in der Regel auch besondere Personenbezogene Daten i. S. v. § 4 Nr. 2 KDG (Gewerkschaftszugehörigkeit, ethnische Herkunft, Gesundheits- und Sexualdaten u.a.).

Aus diesem Grund ist eine Verarbeitung gem. § 4 Nr. 3 KDG (dazu gehören auch Auslesen, Abfragen, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung) nur zulässig, wenn eine entsprechende Einwilligung oder eine gesetzliche Grundlage vorhanden ist. Im Beschäftigungsverhältnis ist § 53 KDG maßgeblich, wonach personenbezogene Daten nur verarbeitet werden dürfen, wenn dies zur Begründung, die Durchführung oder die Beendigung des Beschäftigungsverhältnisses erforderlich ist.

In diesem Sinne hat das BAG bereits 1987 geurteilt:

„Aufgrund des verfassungsrechtlich gewährleisteten Persönlichkeitsschutzes ist der Arbeitgeber verpflichtet, die Personalakten des Arbeitnehmers sorgfältig zu verwahren, bestimmte Informationen vertraulich zu behandeln und für die vertrauliche Behandlung durch die Sachbearbeiter Sorge zu tragen (Fortführung der bisherigen Rechtsprechung des Senats). Auch muss der Arbeitgeber den Kreis der mit Personalakten befassten Mitarbeiter möglichst eng halten.[81]

Damit besteht für den Dienstgeber die Verpflichtung, detailliert zu regeln, wer in welchem Umfang Inhalte der Personalakte zur Kenntnis nehmen darf. Wer berechtigt ist zu einem bestimmten Thema Einblick in die Personalakte zu nehmen ist nicht automatisch berechtigt den Inhalt der gesamten Personalakte zu kennen. Hier ist ein Rechtekonzept zu etablieren. In den Verfahrensverzeichnissen ist darzustellen, welche personenbezogenen Daten für einzelne Verfahren ggf. erforderlich sind und wer diese Daten durch Einsicht in die Personalakte erheben darf.

In keinem Fall ist es ohne Einwilligung des Betroffenen zulässig, die Personalakte für Zwecke einzusehen, für die keine Erforderlichkeit i. S. d. § 53 Abs. 1 KDG besteht. So ist die Herausgabe der Personalakte nicht zulässig, wenn die darin erhaltenen

[81] BAG, Urteil vom 15. Juli 1987 – 5 AZR 215/86

Informationen z. B. für die Erstellung einer Laudatio zum Dienstjubiläum verwendet werden sollen.

4.8. Dashcam Nutzung in Dienstfahrzeugen

Dashcams[82]sind Kameras, die im Fahrzeug, in der Regel auf dem Armaturenbrett angebracht werden, um den Straßenverkehr während der Fahrt zu filmen und aufzuzeichnen. Die Kameras werden teilweise von den Mitarbeitenden in Eigenregie verwendet oder in anderen Fällen vom Dienstgeber zur Verfügung gestellt. Zweck dieser technischen Einrichtung ist es, im Falle eines Verkehrsunfalls die Schuldfrage mit Hilfe der Auswertung des Mitschnitts klären zu können.

Aufsehen hat in diesem Zusammenhang ein Urteil des Bundesgerichtshofes[83]erregt, bei dem es um die Verwertbarkeit solcher Aufzeichnungen ging.

Ein Autofahrer wollte die von seiner Kamera gefertigten Aufzeichnungen nutzen, um dadurch die Schuldfrage eines Unfalls zu klären, in den er verwickelt war. Die beiden Vorinstanzen haben die Verwertbarkeit der Aufzeichnungen abgelehnt.[84] Sie sind dabei davon ausgegangen, dass eine permanente anlasslose Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke des Klägers, zur Wahrnehmung seiner Beweissicherungsinteressen, nicht erforderlich ist. Die Aufzeichnungen verstießen gegen § 4 BDSG a.F., da sie ohne Einwilligung der Betroffenen erfolgt ist und nicht auf § 6b Abs. 1 BDSG a.F. gestützt werden kann. Der BGH bestätigt die Rechtswidrigkeit der permanenten Aufzeichnungen, stellt aber fest, dass im Zivilrechtsverfahren rechtswidrig erlangte Beweismittel mangels einer entgegenstehenden gesetzlichen Regelung dennoch verwertet werden können.

Im Ergebnis ist festzustellen, dass die Verwendung von Dashcams zulässig ist, wenn die von der Kamera gefertigten Aufzeichnungen immer wieder überschrieben werden, bis es zu einem Unfallereignis o.ä. kommt. Der Zeitraum der Aufzeichnungen sollte dabei zwei bis drei Minuten nicht übersteigen. Solche Aufzeichnungen wären dann auch datenschutzrechtlich zulässig.[85]

[82] Zusammengesetzt aus den englischen Wörtern dashboard (Armaturenbrett) und camera
[83] BGH Urteil vom 15. Mai 2018 – VI ZR 233/17
[84] AG Magdeburg – Urteil vom 19. Dezember 2016 – 104 C 630/15 LG Magdeburg – Urteil vom 5. Mai 2017 – 1 S 15/17
[85] Der BGH hat nach Klärung dieser Frage den Fall an das LG Magdeburg zurück verwiesen. Dies hat zwar die Aufzeichnungen verwertet, dem Kläger wurde aber dennoch eine hälftige Mitschuld angelastet.

4.9 GPS-Überwachung von Mitarbeiter-Kfz

Überwachung von Dienstfahrzeugen mittels GPS (Global Positioning System) ist nur unter strengen Voraussetzungen möglich. GPS-Systeme in Dienstfahrzeugen müssen so gestaltet werden, dass eine Überwachung des Mitarbeiters nicht ohne sein Wissen erfolgen kann.

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.

Aber auch wenn das Fahrzeug 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.

Bei der Einführung und Nutzung muss von Seiten der MAV darauf geachtet werden, dass die Zwecke der Verwendung von dabei erfassten Daten konkret und abschließend in Dienstvereinbarungen geregelt werden.

5. Das erweiterte Führungszeugnis

Die Regelungen zur Vorlage des erweiterten Führungszeugnisses sind in den einzelnen Bistümern sehr verschieden ausgestaltet. Sowohl der Kreis der zur Vorlage Verpflichteten als auch das Verfahren mit den Zeugnissen sowie der Umgang mit den daraus gewonnenen Erkenntnissen werden ungleich gehandhabt. Das bewirkt unterschiedlich intensive Eingriffe in die Persönlichkeitsrechte der Mitarbeiter.

5.1. Führungszeugnis und Fragerecht

Bei Begründung eines Arbeitsverhältnisses hat der Arbeitgeber zunächst ein Interesse daran zu erfahren, über welche fachlichen Fähigkeiten der Bewerber verfügt. Dies ist durch Zeugnisse zu belegen. Häufig wird den Arbeitgeber aber auch interessieren, über welche charakterlichen Eigenschaften der Bewerber verfügt. Dies wird er dann durch gezielte Fragen zu erkunden versuchen. Nach den von der Rechtsprechung entwickelten Grundsätzen darf der Arbeitgeber aber nur solche Fragen stellen, an deren Beantwortung er ein berechtigtes und schutzwürdiges Interesse hat.[86] Das Interesse des Arbeitgebers muss so stark sein, dass das berechtigte Interesse des Arbeitnehmers an der Wahrung seines Persönlichkeitsrechtes dahinter zurücksteht.[87]

Nach § 10a Abs. 1 KDO (§ 53 Abs. 1 KDG) dürfen personenbezogene Fragen eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden. Gem. § 2 Abs. 12 Nr. 9 KDO (§ 4 Nr. 24 i KDG) gelten Bewerber als Beschäftigte bzw. werden diesen gleichgestellt. Das gilt gem. § 10a Abs. 2 KDO (§ 53 Abs. 3 KDG) auch für den Fall, dass die Angaben nicht in automatisierten Dateien verarbeitet werden.[88] Stellt der Arbeitgeber Fragen, deren Beantwortung für den angestrebten Arbeitsplatz und die zu verrichtende Tätigkeit selbst nicht von Bedeutung sind, sind diese Fragen unzulässig mit der Folge, dass der Arbeitnehmer diese nicht wahrheitsgemäß beantworten muss. Er hat das Recht zu lügen.[89]

Auch die pauschale Frage nach Vorstrafen ist nach der Rechtsprechung nur insoweit zulässig, als diese für die in Aussicht genommene Tätigkeit „einschlägig“ sind[90]. Diese

[86]Linck in Schaub Arbeitsrechtshandbuch 14. Auflage § 26 Rn. 16
[87] BAG Urteil vom 05.10.1995, 2 AZR 923/94
[88]Däubler Gläserne Belegschaften? 6. Auflage 2015 Rn. 209a
[89]Thüsing in Hensler Willemsen Kalb 7. Auflage 2016 § 123 Rn. 8
[90] Bundesarbeitsgericht, Urteil vom 20.05.1999, AZ: 2 AZR 320/98; Däubler, Gläserne Belegschaften?, Rn. 220; Fitting Kommentar zum BetrVG § 94 Rn. 19

Grundsätze sind auf das Verlangen der Vorlage eines Führungszeugnisses zu übertragen[91].

Eine generelle Forderung des Arbeitgebers zur Vorlage eines Führungszeugnisses ist also unzulässig[92]. Eine solche allgemeine Pflicht zur Vorlage eines Führungszeugnisses würde die von der Rechtsprechung entwickelten Grundsätze zum Fragerecht aushöhlen[93]. Durch die verpflichtende Vorlage eines Führungszeugnisses könnte der Arbeitgeber Kenntnisse erlangen, die ihm gerade durch die Einschränkungen des Fragerechts verwehrt blieben.[94]

Durch eine Gesetzesänderung im Jahr 2009 wurde § 30a Bundeszentralregistergesetz (BZRG) eingeführt,[95] weil Erfahrungen gezeigt haben, dass sich Menschen mit pädophilen Neigungen bewusst Betätigungsfelder gesucht haben, die mit einer Nähe zu Kindern und Jugendlichen verbunden sind.[96]

Um sicher zu stellen, dass Personen die rechtskräftig wegen einer Straftat nach den §§ 171, 174 bis 174c, 176 bis 180a, 181a, 182 bis 184g, 184i, 201a Absatz 3, den §§ 225, 232 bis 233a, 234, 235 oder 236 des Strafgesetzbuchs verurteilt worden sind, nicht im Bereich der Kinder und Jugendarbeit tätig werden, sollen sich die Arbeitgeber zu diesem Zweck bei der Einstellung oder Vermittlung und in regelmäßigen Abständen von den betroffenen Personen ein Führungszeugnis nach § 30 Absatz 5 und § 30a Absatz 1 BZRG vorlegen lassen. § 30a BZRG wurde eingeführt, um das Interesse der Gesellschaft an dem Schutz vor Personen, die insbesondere wegen eines Sexualdeliktes verurteilt wurden, im Bereich des Kinder- und Jugendschutzes zu stärken.[97]

Für die katholische Kirche sind durch die Bischöfe in den einzelnen Bistümern Präventionsordnungen erlassen worden, die die Verpflichtung aus 30 a BZRG, § 72a SGB VIII aufnehmen und fortschreiben.

So wird festgelegt, dass kirchliche Rechtsträger sich bei Einstellung und dann alle fünf Jahre ein erweitertes Führungszeugnis von allen Personen, die im Rahmen ihrer haupt-, neben -oder ehrenamtlichen Tätigkeit Minderjährige oder schutz -oder hilfebedürftige Erwachsene beaufsichtigen, betreuen, erziehen, beraten, ausbilden oder vergleichbaren Kontakt zu ihnen haben, vorlegen lassen. Diese Verpflichtung

[91] Joussen NZA 2012, 777
[92] Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 6. TB 1987, S. 146
[93] Däubler, Gläserne Belegschaften?, Rn. 220;
[94] Ertel, DuD 2012, 126, 128
[95] Fünftes Gesetz zur Änderung des Bundeszentralregistergesetzes vom 16.07.2009 - BGBl I 2009, S. 1952
[96] BT-Drs. 16/12427
[97] BT Drs. 16/12427

gilt regelmäßig auch für Honorarkräfte, Praktikanten, Freiwilligendienstleistende und Menschen in Arbeitsgelegenheiten nach dem SGB II.[98]

5.2. Wer muss ein erweitertes Führungszeugnis vorlegen

Aus datenschutzrechtlicher Sicht fraglich ist nun, welche Mitarbeiter einer Einrichtung zur Abgabe eines erweiterten Führungszeugnisses aufgefordert werden können, wenn dort Minderjährige beschäftigt werden.

Die Regelung des Erzbistums Berlin legt nahe, dass alle Mitarbeiter der Einrichtungen davon erfasst sein sollen.

„*Die Pflicht zur Vorlage eines erweiterten Führungszeugnisses betrifft auch technische und Verwaltungsmitarbeiterinnen und -mitarbeiter, wenn sie aufgrund örtlicher Gegebenheiten Einzelkontakt zu jungen Menschen haben oder habenkönnen, …*“ (§ 5 Abs. 4 Präventionsordnung des Erzbistums Berlin)[99]

Wenn Minderjährige in einer Einrichtung beschäftigt werden, kann nie ausgeschlossen werden, dass diese Kontakt zu jedem Mitarbeiter der Einrichtung „habenkönnen“. Auch wenn von „Einzelkontakten“ gesprochen wird, beschränkt das die Anwendungsbreite nicht.

Die Formulierung in den Präventionsordnungen der anderen Bistümer „..Kontakt … haben“ lässt demgegenüber auch die Interpretation zu, dass nur solche Personen, die üblicher Weise oder regelmäßig Kontakt zu den Minderjährigen haben, verpflichtet sind ein erweitertes Führungszeugnis vorzulegen.[100]

Werden erweiterte Führungszeugnisse von allen Mitarbeitern abverlangt, die in einer Einrichtung tätig sind, die auch Minderjährige beschäftigt, besteht die Gefahr, dass der Arbeitgeber aufgrund der Sonderregelungen der §§ 30a BZRG, 72a SGB VIII Informationen über den Mitarbeiter erhält, die über den Schutzzweck dieser Vorschrift hinausgehen. Durch diese Vorschrift darf nicht über das durch den Gesetzeszweck bedingte Maß hinaus in das Persönlichkeitsrecht des Mitarbeiters eingegriffen werden.

Der Mitarbeiterkreis, von dem ein erweitertes Führungszeugnis abverlangt werden kann, ist durch das BZRG bewusst eng gehalten. Danach ist das erweiterte Führungszeugnis als zielgerichtete Maßnahme für alle kinder- und jugendnahen Tätigkeiten eingerichtet worden. Der Gesetzgeber hat sich bewusst dagegen

[98] Z. B. §§ 5 Abs. 1, 2 Abs. 7 der Präventionsordnungen der Bistümer Dresden-Meißen, Erfurt, Görlitz und Magdeburg
[99] Die Formulierung „…haben können..“ findet sich auch in den Präventionsordnungen der Bistümer Münster, § 2 Abs. 3; Hildesheim, § 5 Abs. 3; Limburg, § 2 Abs. 2
[100] So ausdrücklich z. B. Bistum Freiburg, § 6 Abs.1

entschieden, den Straftatenkatalog für alle Führungszeugnisse auszuweiten, unabhängig von der in Blick genommenen Tätigkeit.[101]

Deshalb ist es unzulässig, alle Mitarbeiter eines Trägers der Kinder- und Jugendarbeit zur Abgabe eines erweiterten Führungszeugnisses zu verpflichten. Vielmehr kann die Vorlage nur dann verlangt werden, wenn der entsprechenden Person konkret eine in der Präventionsordnung genannte Tätigkeit übertragen werden soll. Tätigkeiten, die nur punktuell oder eher zufällig zum Kontakt mit Kindern oder Jugendlichen führen, fallen nicht darunter.[102] So ist die Anforderung eines erweiterten Führungszeugnisses für eine/n Büroangestellte/n der Kontakt mit einem Minderjährigen haben könnte unverhältnismäßig.[103] Die Anforderung eines erweiterten Führungszeugnisses für einen Hausmeister, der an einer Schule oder einem Kindergarten tätig ist, ist erforderlich,[104] Eine solche Anforderung für den Hausmeister eines Ordinariates aber nicht. Es ist immer zu prüfen, ob ein Mitarbeiter durch seine Tätigkeit typischer Weise eine Nähe zu Kindern und Jugendlichen entwickelt, die ihm eine besondere Gelegenheit bietet, eine der im Gesetz genannten Straftaten zu Lasten der Kinder oder Jugendlichen zu begehen.[105] Nur diese Fälle sind von der Intention des Gesetzgebers erfasst.

5.3. Verfahren mit dem erweiterten Führungszeugnis

In einigen (Erz-)Bistümern legen die Präventionsordnungen ausdrücklich fest, dass das erweiterte Führungszeugnis der „Personalakten führenden Stelle“ vorzulegen ist.[106]

§ 30 Abs. 4 BZRG legt fest, dass das Führungszeugnis nur an die beantragende Person übersendet werden darf. Diese soll also selbst entscheiden können, ob und wem sie das Zeugnis vorlegt. Nach dem BZRG gibt es kein „Arbeitgeberführungszeugnis“, welches sich auf die Darstellung der Eintragungen beschränkt, die einen konkreten Bezug zu dem Arbeitsverhältnis haben. So beinhaltet auch das erweiterte Führungszeugnis gem. § 30 a BZRG über die Angaben gem. § 72 a SGB VIII hinaus alle Angaben, die in einem einfachen Führungszeugnis gem. § 30 BZRG enthalten sind. Damit geht die Information des erweiterten Führungszeugnisses ggf. deutlich über den Zweck, der mit seiner Anforderung erreicht werden sollte, hinaus.

[101] Begründung des Gesetzesentwurfs BT-Drs. 16/12427
[102]Tolzmann Bundeszentralregistergesetz 5. Auflage 2015 § 30a Rn. 8
[103]Tolzmann Bundeszentralregistergesetz 5. Auflage 2015 § 30a Rn. 11
[104] Begründung zum Gesetzentwurf des BZRG Besonderer Teil zu § 30 a Abs.1 BT-Drs. 16/12427
[105]Joussen NZA 2012, 779
[106] Z.B. (Erz-)Bistümer Münster, § 4 Abs. 1; Speyer, § 4 Abs.1; Hildesheim, § 6 Abs.1; Bamberg § 4 Abs. 1

Aus datenschutzrechtlicher Sicht ist die Vorlage eines erweiterten Führungszeugnisses aber nur dann erforderlich, wenn es keinen anderen Weg gibt, die Vorschriften der Präventionsordnung bzw. des § 72 a SGB VIII nach Sinn und Zweck zu erfüllen.

Es besteht die Möglichkeit, durch Einschalten einer Amtsperson, die Persönlichkeitsrechte des Mitarbeiters zu wahren und gleichzeitig den Zweck der gesetzlichen Regelungen zu erfüllen. Dies könnte dadurch geschehen, dass der Mitarbeiter sein Führungszeugnis einem Notar vorlegt, und dieser bestätigt, dass dort Straftaten bzw. Verurteilungen gem. § 72a SGB VIII nicht enthalten sind.

Ebenfalls denkbar wäre die Vorlage des Führungszeugnisses beim Präventionsbeauftragten oder einem anderen zur Verschwiegenheit verpflichteten Mitarbeiter der Einrichtung, wenn ausgeschlossen ist, dass dieser mit Personalentscheidungen in der Einrichtung, gleich in welchem Stadium, zu tun hat.[107]

Da auf diesem Weg der Gesetzeszweck erreicht werden kann, ist das Verlangen zur Vorlage eines erweiterten Führungszeugnisses, welches auch Eintragungen enthalten kann, die mit dem Zweck nicht in Zusammenhang stehen, an die Personalakten führende Stelle nicht erforderlich und damit unzulässig.

5.4. Umgang mit Führungszeugnissen

In der Regel ist in den Präventionsordnungen festgelegt, dass die Führungszeugnisse in einem „verschlossenen“ Umschlag der Personalakte beigefügt werden.[108] Datenschutzrechtlich ist eine derartige Verfahrensweise abzulehnen, da dieses Verfahren keinen hinreichenden Schutz gegen unberechtigte Kenntnisnahme bietet. Es nicht besonders hinderlich ist, einen Umschlag zu öffnen und seinen Inhalt in einem neuen Umschlag zu verschließen. Erst recht abzulehnen ist die unverschlossene Abheftung in der Personalakte.[109] Ein Schutz gegen die unberechtigte Kenntnisnahme kann erreicht werden, indem das erweiterte Führungszeugnis in einem versiegelten Umschlag aufbewahrt wird[110] oder in separat zu führenden verschlossenen Unterlagen.[111]

Tatsächlich stehen aber die vorgenannten Verfahren insgesamt in Widerspruch zum Datensparsamkeitsgebot des § 2a KDO (§ 7 Abs. 1 c KDG). Danach ist die

[107] Erzbistum Berlin § 6 Abs.4; Bistum Limburg Ausführungsbestimmungen zur Präventionsordnung II.3.
[108] Z. B. Bistümer Münster, § 4 Abs. 1; Bistum Hildesheim § 6 Abs. 1; Erzbistum Bamberg, § 4 Abs.1
[109] Bistum Speyer § 4 Abs. 1
[110] Z.B. Bistum Augsburg, § 8 Abs. 1;
[111] Bistum Limburg, Ausführungsbestimmungen zur Präventionsordnung III.8.

Verarbeitung von Daten nur dann zulässig, wenn dies erforderlich ist. Nach § 72 a Abs. 5 SGB III ist nur der Umstand, dass Einsicht in ein Führungszeugnis genommen wurde, das Datum des Führungszeugnisses und die Information, ob die das Führungszeugnis betreffende Person wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist, festzuhalten. Für die Aufnahme des Führungszeugnisses selber besteht keine Erforderlichkeit. Datenschutzkonform sind insoweit nur die Präventionsordnungen der (Erz-)Bistümer Berlin und Würzburg, in denen festgelegt ist, dass die erweiterten Führungszeugnisse nach Einsichtnahme an die betreffenden Mitarbeiter zurückgegeben werden.[112]

5.5. Umgang mit Eintragungen die über Erkenntnisse des § 72a SGB VIII hinausgehen

Abschließend bleibt die Frage zu klären, wie ggf. damit umzugehen ist, wenn das erweiterte Führungszeugnis Eintragungen enthält, die mit dem Zweck des § 72a SGB VIII nicht in Zusammenhang stehen. Eine Präventionsordnung legt fest: „Bei vorliegenden Eintragungen von Vorstrafen ist unverzüglich der Generalvikar … zu informieren“.[113]

Hier gilt: Der Arbeitgeber darf die Daten nur für die Zwecke verwenden, für die er sie erhoben hat (§10 Abs. 1 KDO; § 6 Abs. 2 KDG). Auch § 72a V SGB VIII weist ausdrücklich auf die Zweckbindung der Datenerhebung hin.

Die im erweiterten Führungszeugnis mitgeteilten Daten werden zur Erfüllung der gesetzlichen Verpflichtungen aus Präventionsordnung und SGB erhoben. Zweck der Erhebung ist der Tätigkeitsausschluss einschlägig vorbestrafter Personen und nicht eine allgemeine Überprüfung des Mitarbeiters. Aus diesem Grunde ist die Verwendung von Eintragungen, die keinen Bezug zur Präventionsordnung oder zu § 72a SGB VIII haben, aber dennoch im erweiterten Führungszeugnis erwähnt werden, sog. „Beifang“, unzulässig.[114]

5.6. Zusammenfassung

Die Präventionsordnungen der Bistümer sollten entsprechend den datenschutzrechtlichen Regelungen überarbeitet werden. Insbesondere im Hinblick

[112] Bistum Würzburg, § 4 Abs. 3; Erzbistum Berlin § 6 Abs.1
[113] Bistum Mainz § 3 Abs. 2
[114] Ausdrücklich wird dies nur in den Präventionsordnungen der (Erz-)Bistümer Berlin, § 6 Abs. 4; Augsburg, § 8 Abs. 3; sowie in den Ausführungsbestimmungen zur Präventionsordnung im Bistum Limburg III.7. und in der Handreichung zur Präventionsordnung des Bistums Würzburg S. 8 dargestellt.

auf den Mitarbeiterdatenschutz muss gewährleistet werden, dass der Kreis der zur Vorlage eines erweiterten Führungszeugnisses Verpflichteten auf die Mitarbeiter beschränkt bleibt, die regelmäßig mit den zu schützenden Personengruppen zusammenarbeiten. Mit der Kenntnisnahme der Inhalte der Führungszeugnisse sind ausschließlich Personen zu beauftragen, die in keinerlei Personalentscheidung eingebunden sind. Führungszeugnisse sind lediglich einzusehen und im Sinne der Datensparsamkeit nach Einsichtnahme an die Betroffenen zurück zu geben. Es ist deutlich zu regeln, dass bezüglich der weiteren Erkenntnisse, die aus einem erweiterten Führungszeugnis ersichtlich werden, ein Verwertungsverbot besteht.

6. Besondere Problembereiche

6.1. Facebook Fanpages

Die Konferenz der Diözesandatenschutzbeauftragten hat sich mit Beschluss vom 10. Oktober 2018 erneut dafür ausgesprochen auf das Betreiben einer Facebook-Fanpage zu verzichten, da eine datenschutzrechtliche Haftung des Betreibers einer Fanpage nicht wirksam ausgeschlossen werden kann. Dieser Beschluss knüpft an die Empfehlung der Diözesandatenschutzbeauftragten vom 26. Juli 2018 an, dass die Grundsätze der Datenschutzkonferenz des Bundes und der Länder (DSK) zum EuGH-Urteil vom 05.06.2018 ebenso für kirchliche Einrichtungen gelten, welche eine Fanpage bei Facebook betreiben.

Die Betreiber einer solchen Homepage auf dem Portal von Facebook müssen aufgrund der Vorschrift des § 28 KDG Auskunft darüber geben können, zu welchen Zwecken und auf welcher Rechtsgrundlage die personenbezogenen Daten der Besucher von Fanpages verarbeitet werden und welche personenbezogenen Daten gespeichert werden. Auch müsste der Betreiber angeben inwieweit aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert werden. Weiterhin müsste dargestellt werden, ob und wie personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet werden.

Der EuGH stellt fest, dass Facebook und der Seitenbetreiber gemeinschaftlich haften. Nach der Regelung des Art. 26 DSGVO (§28 KDG) betreiben nämlich Facebook und der Verwender einer Facebook Fanpage auf Augenhöhe als gemeinsame Verantwortliche die Seite. Für etwaige Datenschutzrechtsverletzungen sind sie deshalb auch gemeinschaftlich verantwortlich. Dabei spielt es keine Rolle, dass bei realistischer Betrachtung kein Seitenbetreiber mit dem Weltkonzern Facebook auf Augenhöhe zusammenarbeitet, da er nicht einmal eine Möglichkeit hat diese

Datensammlung abzuschalten. An diesem Umstand hat Facebook bis heute nichts geändert. Völlig absurd ist es, wenn Facebook den Seitenbetreiber verpflichtet, DSGVO-konform zu arbeiten, auch wenn ihm die faktische Möglichkeit in jeder Hinsicht verwehrt wird und nur Facebook bestimmen kann, welche Daten gesammelt und wie sie verarbeitet werden. Und nur Facebook alleine weiß, zu welchen Zwecken und aus welchem Rechtfertigungsgrund.

Unter den derzeitigen Bedingungen, die von Facebook festgelegt sind, ist eine rechtskonforme Nutzung der Facebook Fanpage nicht möglich!

6.2. Fotos

Ein Foto fällt unter die Definition personenbezogener Daten. Durch das Foto werden Auskünfte über eine bestimmte Person gegeben, die über das bloße Aussehen hinausgehen. So kann z. B. das Alter (zumindest ungefähr), ein Migrationshintergrund, das Geschlecht, eine Behinderung, ggf. die Religion o.ä. erkannt werden. Aber auch die Stimmung in der sich der Fotografierte befindet sowie häufig seine örtliche und soziale Umgebung. Niemand muss es hinnehmen, dass diese Daten über ihn erhoben werden. Deshalb muss auch niemand akzeptieren fotografiert zu werden. Aus Sicht des Fotografen heißt das, er muss vor der Aufnahme einer Person deren Erlaubnis einholen, ein Foto zu machen.

Eine solche Erlaubnis kann auch konkludent, also durch schlüssiges Verhalten, erteilt werden. Das betrifft jedoch zunächst nur die Erlaubnis ein Foto aufzunehmen. Wer freundlich in die Kamera lächelt gibt dem Fotografen zu verstehen, dass er mit der Ablichtung einverstanden ist. Mehr aber auch nicht!

Herstellung, Verschaffung oder Besitz eines Bildnisses für das keine Rechtsgrundlage besteht, stellen auch dann eine Verletzung des allgemeinen Persönlichkeitsrechtes dar, wenn keine Verbreitungsabsicht besteht.[115]

Die Erstellung von Fotos richtet sich also nach den Regeln des Datenschutzes, da es sich um die Verarbeitung personenbezogener Daten handelt.

Personenbezogene Daten sind gem. § 4 Nr. 1 KDG alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Damit fallen zunächst all diejenigen Bilder unter diese Kategorie, auf denen Betroffene direkt zu erkennen sind, weil ihr Gesicht erkennbar ist. Identifizierbarkeit kann aber auch dann gegeben sein, wenn zwar nicht das Gesicht von Personen abgebildet ist, jedoch aufgrund anderer erkennbarer Merkmale auf eine bestimmte Person geschlossen werden kann. In einem unserer Dienststelle vorgelegten Fall ging es um die Abbildung

[115]LG Aschaffenburg Urteil vom 31.10.2011 – 14 O 21/11, NJW 2012, 287

einer Person in einer Kirche. Die Person saß in der ersten Reihe, in der ansonsten leeren Kirche am Gründonnerstag, wie sich aus der Bildunterschrift ersehen ließ. Die Person trug eine individuelle besonders markante selbstgestrickte Mütze. Da die Person diese Mütze regelmäßig trägt und auch in der Pfarrei bekannt ist, dass die namentlich bekannte Person diese Mütze trägt, war die Person auf dem Foto individualisierbar. Dabei kommt es nicht darauf an, dass die Identifizierbarkeit nur einem eingeschränkten Personenkreis, in dem Fall dem Großteil der Pfarreimitglieder, möglich war. Das Recht am eigenen Bild ist bereits dann verletzt, wenn der Abgebildete begründeten Anlass hat, er könne identifiziert werden.[116]

Die Veröffentlichung des Fotos auf der Homepage der Pfarrei war deshalb unzulässig.

6.2.1. Verwendung von Fotos im Kontext mit Kindern und Jugendlichen

Insbesondere Einwilligung von Kindern und Jugendlichen nach dem KDG und der DSGVO

Eine einheitliche Definition von Jugendlichen oder Kindern gibt es im deutschen Recht nicht. Jedoch bezeichnet das Jugendgerichtsgesetz als Jugendliche Minderjährige zwischen 14 und 18 Jahren. Wer noch nicht 14 Jahre alt ist, wird als Kind bezeichnet.[117]

Die DSGVO macht demgegenüber keine Unterscheidung zwischen Jugendlichen und Kindern. In der Verordnung wird durchgehend von Kindern gesprochen. Art 8 Abs. 1 DSGVO bringt dennoch eindeutig zum Ausdruck, dass mit dem Begriff „Kinder“ alle Personen unter 18 Jahren gemeint sind. Das KDG spricht in § 8 Abs. 8 von Minderjährigen.[118] Es geht nachfolgend also um die Einwilligung von unter 18-jährigen Personen unabhängig von der Bezeichnung in den jeweiligen Normen.

Indem die DSGVO in Art. 8 und in Erwägungsgrund 65 S. 2 ausdrücklich die Möglichkeit der Einwilligung von Kindern anspricht, ist festgestellt, dass Geschäftsfähigkeit i. S. d. Bürgerlichen Gesetzbuches für die Einwilligung nicht erforderlich ist.[119]

Die DSGVO legt kein Mindestalter fest, ab dem eine Einwilligung durch einen Minderjährigen wirksam abgegeben werden kann. Lediglich in Artikel 8 Abs. 1 DSGVO, § 8 Abs. 8 KDG wird für den Fall des Angebotes von Diensten der

[116] BGH Urteil vom 26.01.1971, NJW 1971, 698, 700
[117] § 1 Abs. 2 JGG
[118] Ebenso das DSG-EKD (Datenschutzgesetz der evangelischen Kirche) in § 12
[119] Ernst in Paal/Pauly Art. 4 Rn. 66; Schwartmann/Hilgert in Heidelberger Kommentar Art. 8 Rn. 11

Informationsgesellschaft das einem Kind direkt gemacht wird, für die Wirksamkeit der Einwilligung ein Mindestalter von 16 Jahren gefordert.[120] Diese Altersregelung bezieht sich ausschließlich auf den benannten Anwendungsbereich. Eine generelle Voraussetzung für die Einwilligungsfähigkeit von Minderjährigen ist damit nicht festgeschrieben.[121] Insoweit ist keine Änderung durch die Verordnung gegenüber der davor geltenden Richtlinie[122] für solche Sachverhalte erfolgt, die Einwilligungen in Sachverhalte außerhalb dieser Vorschrift betrifft. Wie bislang im deutschen Recht kann deshalb auch weiterhin davon ausgegangen werden, dass die Wirksamkeit der Einwilligung eines Minderjährigen von dessen Einsichtsfähigkeit abhängt.[123]Also davon, ob der Minderjährige psychisch und intellektuell in der Lage ist, Bedeutung und Tragweite seiner Entscheidung einzuschätzen. Diese Sichtweise wird auch durch den Erwägungsgrund 58 gestützt. Abstrakte Aussagen, wann eine Einsichtsfähigkeit gegeben ist, insbesondere die Knüpfung an ein bestimmtes Alter, scheiden also aus.[124] Bestenfalls als ein Anhaltspunkt kann ab einem Alter von 14 bis 15 Jahren in der Regel vermutet werden[125], dass die Einsichtsfähigkeit gegeben ist, was jedoch nicht von einer Einzelfallprüfung entbindet.[126]Fehlt die Einsichtsfähigkeit, bedarf es der Einwilligung der Erziehungsberechtigten, liegt Einsichtsfähigkeit vor, ist eine doppelte Einwilligung sowohl des Minderjährigen als auch der Erziehungsberechtigten erforderlich.

Das Recht auf informationelle Selbstbestimmung ist als ein an eine bestimmte Person gebundenes Recht, das wegen seines besonderen Charakters im Grundsatz weder übertragbar noch vererblich ist,[127] ein höchstpersönliches Recht. Damit muss grundsätzlich auch eine Einwilligung in Bezug auf ein solches Recht höchstpersönlich erklärt werden.[128] Ausnahme von diesem Grundsatz ist die Abgabe der Einwilligungserklärung der Sorgeberechtigten für ihr Kind.[129] Das Recht auf informationelle Selbstbestimmung ist nach der grundlegenden Entscheidung des Bundesverfassungsgerichtes zum Volkszählungsurteil selber ein Grundrecht.[130] Das Einwilligungsrecht der Eltern in dieses Grundrecht ihrer Kinder können die Eltern nur

[120] Nach § 12 DSG-EKD Mindestalter 14 Jahre.
[121]Kampert in Sydow Europäische Datenschutzgrundverordnung Art. 8 RN. 7; Schwartmann/Hilgert in Heidelberger Kommentar Art. 8 Rn. 10
[122] EU DSRL 95/46/EG vom 24.10.1995
[123]Kampert in Sydow Europäische Datenschutzgrundverordnung Art. 8 RN. 7
[124] Simitis Kommentar zum BDSG § 4a Rn. 21
[125] 40. TB Hessischer Datenschutzbeauftragter
[126] Ernst, DANA 2017, 14
[127]Duden Recht A-Z. Fachlexikon für Studium, Ausbildung und Beruf. 3. Aufl.
[128] Simitis Kommentar zum BDSG § 4a Rn. 30; Weichert in DKWW Kommentar zum BDSG § 4a Rn. 6; Paal/Pauly Kommentar zur DSGVO Art. 4 Rn.65; 46. TB Hessischer Datenschutzb. S. 108
[129] Ernst DANA 2017, 14
[130] BVerfGE 65, 1ff.

selber ausüben. Ein Verzicht darauf ist nicht möglich.[131] Eine willkürliche Übertragung dieses Rechtes an Dritte scheitert an der Höchstpersönlichkeit dieses Rechtes, bzw. daran, dass es sich hierbei um eine wesentliche Angelegenheit i. S. d. § 1687 I BGB handelt.[132] So ist insbesondere die Übertragung des Sorgerechts im Hinblick auf die Anfertigung von Bild- und Tonaufnahmen auf einen Dritten nicht möglich. Dies muss umso mehr gelten, wenn der Dritte damit eigene Interessen verfolgt. Dies dürfte bei der Anfertigung von Fotos oder Videoaufnahmen durch Kindergärten, Schulen und bei Ferienfreizeiten der Fall sein, da diese zumindest auch der Werbung für diese Einrichtung dienen. Insoweit dürfte ein Interessenkonflikt bei den Beauftragten bestehen.

Eine pauschale Generaleinwilligung für alle gleichgelagerten Fälle für die Dauer der Zugehörigkeit des Minderjährigen in einer Einrichtung ist grundsätzlich unzulässig. Dies wird insbesondere Einwilligungen zur Erstellung von Fotos und deren Veröffentlichung betreffen, die bei Aufnahme in die KITA oder die Schule für die gesamte Aufenthaltszeit erteilt werden. Art 4 Nr. 11 DSGVO wie auch § 8 Nr. 13 KDG definieren „Einwilligung“ als eine Willensbekundung in informierter Weise für einen bestimmten Fall. Eine informierte Einwilligung dürfte in der pauschalen Einwilligung für die Veröffentlichung aller Fotos während der gesamten Aufenthaltsdauer kaum anzunehmen sein.[133] Außerdem kann unter einem „bestimmten Fall“ nicht die Anfertigung von Fotos gemeint sein, sondern nur die Anfertigung und Veröffentlichung eines konkreten, eben bestimmten Fotos.[134]

Eine Veröffentlichung liegt vor, wenn Daten einer nicht genau feststehenden Mehrzahl von Adressaten, die Dritte sind, zugänglich gemacht werden.[135]Sind die Personen miteinander oder mit dem Veranstalter bekannt, gehören sie nicht zur Öffentlichkeit.[136] Bei KITA´s dürfte deshalb keine Veröffentlichung darin zu sehen sein, wenn Bilder von Kindern innerhalb der Einrichtung ausgehängt werden.[137] Für diese Fälle ist von der ausnahmsweisen Zulässigkeit einer Generaleinwilligung auszugehen. Dies betrifft aber ausdrücklich nur den Innenbereich der Einrichtung im Rahmen der Zweckbindung. Aushänge in Schaukästen oder Veröffentlichung in Flyern sind von dieser Ausnahme nicht umfasst.[138] Für Schulen trifft dies nicht in

[131] Palandt Kommentar zum BGB § 1626 RN. 3
[132] So im Ergebnis auch Hoffmann, JAmt 2015, 8
[133] 46. TB hessischer Landesbeauftragte für Datenschutz S. 109
[134] Welche Blüten eine generelle Einwilligung treibt, ist in dem Formular (Anlage) zu entnehmen, was meiner Dienststelle von der Schulverwaltung eines Bistums zur Genehmigung vorgelegt worden ist.
[135] Dammann in Simitis Kommentar zum BDSG § 3 Rn. 157
[136] § 15 Abs. 3 UrhG
[137] Caritasverband für das Bistum Trier e.V. Arbeitshilfe Datenschutz in kath. Tageseinrichtungen für Kinder
[138] Ministerium für Kultus, Jugend und Sport Baden-Württemberg Datenschutzbroschüre Datenschutz in Kindertageseinrichtungen S. 16; Gutenkunst/Fachet Merkblatt für den Datenschutz in evangelischen und katholischen Kindertageseinrichtungen S. 7

gleicher Weise zu, da der Kreis der Dritten, die Zugang zu der Einrichtung haben, nicht wie bei Kindereinrichtungen überschaubar ist.

Das in der Anlage beigefügte Formular zur „Einwilligung zur Veröffentlichung personenbezogener Daten“ wurde durch die Schulabteilung eines Bistums für die Verwendung in den Schulen dieses Bistums zur Verfügung gestellt. Eine Einwilligung zu diesem Formular kommt einem Verzicht auf das Recht auf informationelle Selbstbestimmung gegenüber dem Schulträger gleich. Ein solcher Verzicht auf Grundrechte ist zumindest dann nicht möglich, wenn das Grundrecht über den einzelnen hinaus auch der Gemeinschaft zugutekommt. Nach Auffassung des Bundesverfassungsgerichts ist die Entfaltung der Persönlichkeit zu gewährleisten, weil Selbstbestimmung eine elementare Funktionsbestimmung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist.[139]

Zusammenfassung:

1. Eine Einwilligung des Minderjährigen ist unabhängig von dessen Geschäftsfähigkeit.
2. Eine Einwilligung kann durch den Minderjährigen erteilt werden, sobald er über die erforderliche Einsichtsfähigkeit verfügt.
3. Vor Vollendung des 18. Lebensjahres wird regelmäßig eine Doppeleinwilligung des Minderjährigen und dessen Sorgeberechtigten erforderlich sein.
4. Aufgrund der Höchstpersönlichkeit der Einwilligung ist eine Vertretung nicht möglich. Ebenso eine willkürliche Weitergabe des Sorgerechts im Wege einer Vertretungsvollmacht an Dritte.
5. Ein Verzicht auf das Recht auf informationelle Selbstbestimmung ist nicht möglich.

6.2.2. Verwendung von Fotos im Arbeitsrecht

Auf der Webseite einer Einrichtung wurde ein Foto von der Haussegnung veröffentlicht. Auf diesem Foto waren zwei Mitarbeitende formatfüllend zu sehen. Einer der beiden wehrt sich gegen diese Darstellung und fragt an, ob der Dienstgeber ohne seine Einwilligung eine solche Abbildung ins Netz stellen darf.

Fotos des Betriebsausfluges wurden im hauseigenen Intranet der Einrichtung veröffentlicht. Auch hier wandten sich Mitarbeitende gegen die Einstellung von Fotos auf denen sie zu erkennen waren.

[139]BVerfGe 65, 1ff.

In einem anderen Fall fordert eine Einrichtung ihre Mitarbeiter dazu auf, Porträtfotos anfertigen zu lassen, damit das Telefonverzeichnis auf der Internetseite des Unternehmens mit diesen Bildnissen versehen werden kann. Dies wird damit begründet, dass diese Form einem modernen Informationsangebot entspräche und auch von anderen Unternehmen so gehandhabt werde.

Werden keine Fotos eingereicht, verwendet der Arbeitgeber die Fotos aus der Personalakte.

6.2.2.1. Anwendbarkeit des Kunsturhebergesetzes überholt

Als Rechtsgrundlage für die Veröffentlichung von Fotos konnte sich das BAG in der zitierten Entscheidung auf die Regelungen in §§ 22 ff. Kunsturhebergesetz (KUG) berufen, die aufgrund § 3 BDSG a.F. als Spezialgesetz gegenüber dem BDSG a.F. vorrangig zur Anwendung kamen.

Die neuen datenschutzrechtlichen Normen bestimmen aber den Anwendungsvorrang der DSGVO vor dem BDSG n.F.[140] Damit ist auch eine Anwendbarkeit des KUG überholt. Zwar hat das OLG Köln in einer Entscheidung die Weitergeltung des KUG festgestellt, diese bezog sich aber lediglich auf Sachverhalte im journalistisch redaktionellen Zusammenhang.[141] Der Sache nach passt diese Öffnungsklausel aber nicht auf den Bereich des Beschäftigungsverhältnisses. Dies wird in § 26 BDSG n.F. (§ 53 KDG; § 49 DSG-EKD) geregelt. Eine Fotoerlaubnis direkt auf der Grundlage dieser Vorschrift ist nur rechtmäßig, wenn dies im Rahmen der Begründung, Durchführung und Beendigung des Arbeitsverhältnisses erforderlich ist. Das dürfte der Fall sein, soweit es um die Anfertigung von Fotos für Dienstausweise u. ä. geht.

Sollte dies nicht zutreffen, richtet sich die Rechtmäßigkeit einer Veröffentlichung nach den Vorschriften des Art 6 DSGVO (§ 6 KDG, § 6 DSG-EKD). Danach ist die Verarbeitung personenbezogener Daten grundsätzlich unzulässig, soweit nicht eine Einwilligung oder eine andere dort benannte Rechtsgrundlage besteht.

6.2.2.2. Berechtigtes Interesse des Arbeitgebers

Als Rechtsgrund für die Abbildung eines Fotos käme Artikel 6 Abs. 1 lit. f) in Betracht, wenn die Veröffentlichung zur Wahrung eines berechtigten Interesses des Arbeitgebers erforderlich wäre und Interessen oder Grundrechte des Betroffenen nicht entgegenstehen.

[140] BDSG n.F. § 1 Abs. 5

[141] OLG Köln Beschluss vom 18.06.2018 - 15 W 27/18: Artikel 85 DSGVO erlaubt … nationale Gesetze mit Abweichungen von der DSGVO zugunsten der Verarbeitung zu journalistischen Zwecken. Er enthält damit eine Öffnungsklausel …

Das berechtigte Interesse des Verantwortlichen wird regelmäßig darin bestehen, eine Öffentlichkeit über Veranstaltungen zu informieren und einen Einblick in das Leben der Einrichtung zu gewähren. Wenn dieses berechtigte Interesse auf anderem Wege gleichermaßen zu befriedigen wäre und dabei die Rechte der Betroffenen weniger beeinträchtigt werden, fehlt es bereits an der Erforderlichkeit.[142] Bei der formatfüllenden Abbildung einzelner Personen oder Gruppen ist fraglich, ob das berechtigte Interesse, also der Zweck, des Verantwortlichen damit befriedigt wird. Auf jeden Fall ist es aber nicht erforderlich im Sinne von notwendig, einzelne Personen erkennbar darzustellen oder zum Hauptgegenstand des Bildes zu machen. Vielmehr können Fotos auch so gestaltet werden, dass ein Eindruck von Veranstaltungen entsteht, ohne dass einzelne Personen erkennbar sind. Selbst wenn man die Erforderlichkeit in diesen Fällen bejahen sollte, scheitert eine Zulässigkeit der Veröffentlichung an der Interessenabwägung, da die betroffene Person durch die Veröffentlichung ihrer personenbezogenen Daten in ihren Grundrechten betroffen ist, weil die Kontrolle über ihre Daten zumindest eingeschränkt, wenn nicht entzogen wird[143] (s.u.).

Die Veröffentlichung von personenbezogenen Daten im Internet kann als erforderlich angesehen werden bei Personen, deren Tätigkeit nach außen wirkt. Angaben, die im Zusammenhang mit einer nach außen gerichteten Tätigkeit als Amtsträger stehen, sind Name, Funktion sowie dienstliche Erreichbarkeit und Dienstort. Die Veröffentlichung dieser Daten ist für die Durchsetzung des berechtigten Interesses des Verantwortlichen erforderlich.[144]Die Abbildung von Fotos, z. B. für das Telefonverzeichnis ist demgegenüber nicht erforderlich, da für die Erreichbarkeit oder die Aufgabenerfüllung der Einrichtung das Aussehen ihrer Mitarbeiter nicht maßgeblich ist.[145] Eine Veröffentlichung von Fotos auch für diesen Zweck bedarf der Einwilligung der Betroffenen. Die Verwendung eines in der Personalakte vorhandenen Fotos ist unzulässig, weil der Zweck zu dem das Bild ursprünglich eingereicht worden ist, nicht die Veröffentlichung im Telefonverzeichnis gewesen ist. Der Verstoß gegen die Zweckbindung des Art. 5 Abs. 1 lit. b) DSGVO (§ 7 Abs. 1 lit. b) KDG, § 7 Abs. 1 DSG-EKD) führt zur Unrechtmäßigkeit der Veröffentlichung.

Bei einer Veröffentlichung im Intranet wird das Bildnis nur einem beschränkten Personenkreis zugänglich gemacht. Jedoch liegt darin eine Verarbeitung gem. Art. 4

[142]Schantz in Simitis Datenschutzrecht Art 6 Abs. 1 Rn. 100
[143] Ehmann/Selmayr/HeberleinKommtar zur DSGVO Art 6 Rn. 34
[144]LfD Niedersachsen “Personaldaten im Internet”, LfD Hessen 25. TB Punkt 8.3.
[145] Im Ergebnis auch Gola/Pötters/Wronka Handbuch Arbeitnehmerdatenschutz Rn. 985

Nr. 2 DSGVO (§ 4 Nr. 3 DSG-EKD; § 4 Nr. 3 KDG) in Form der Offenlegung[146], so dass sich für die rechtliche Beurteilung nichts anderes ergibt.

6.2.2.3. Einwilligung

Nach § 26 Abs. 2 BDSG n. F. (§ 49 DSG-EKD) ist eine Einwilligung auch im Rahmen eines Arbeitsverhältnisses möglich. Diese Frage war nach der alten Rechtslage umstritten.[147] Im KDG fehlt ein solcher ausdrücklicher Hinweis. Jedoch ist auch für den Bereich des KDG sowohl auf Grundlage des Einklangs mit staatlichem Recht als auch aufgrund der Rechtsprechung des BAG[148] zu dieser Frage, von der grundsätzlichen Zulässigkeit einer Einwilligung im Arbeitsverhältnis auszugehen.

Die Einwilligung muss zunächst freiwillig erfolgen. Bei der Beurteilung der Freiwilligkeit einer Einwilligung im Rahmen eines Beschäftigungsverhältnisses ist jedoch die grundsätzlich bestehende Abhängigkeit im Über- Unterordnungsverhältnis zu berücksichtigen. Freiwilligkeit soll u. a. insbesondere vorliegen können, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Mitarbeitende die gleichen Interessen verfolgen.[149] Nach der Begründung zum Gesetzesentwurf des BDSG kann ein gleiches Interesse z. B. bei Nutzung von Fotos für das Intranet vorliegen, bei denen Arbeitgeber und Beschäftigter im Sinne eines betrieblichen Miteinanders zusammenwirken.[150] Das gilt also nur für solche Fotos, bei denen nicht einzelne Mitarbeitende im Vordergrund stehen, sondern das Miteinander.[151]

Liegt weder ein rechtlicher oder wirtschaftlicher Vorteil für den Arbeitnehmer vor, noch ein gleichgelagertes Interesse, wird die Einwilligung dadurch nicht zwingend unwirksam.[152] Vielmehr macht die Formulierung „insbesondere“ deutlich, dass in den benannten Fällen eine gesetzliche Vermutung für die Freiwilligkeit besteht.[153] Das rechtfertigt jedoch nicht den Umkehrschluss, in allen anderen Fällen bestehe diese nicht.[154] Richtig ist aber, dass in diesen Fällen die Umstände des Einzelfalls in besonderer Weise zu berücksichtigen sind, wie z. B. der Zeitpunkt der Einwilligungserteilung.[155] Eine Einwilligung im Zusammenhang mit dem Abschluss

[146] Für das Teilen von Bildern in einer WhatsApp-Gruppe LG Frankfurt Beschluss vom 28.05.2015 – 2-03 O 452/14
[147] Simitis BDSG a. F. § 4 Rn. 7; Täger BDSG a. F. § 4a Rn.; BT-Drs. 17/4230; a. A. Däubler BDSG a. F. § 4a Rn. 24; Thüsing/Traut Beschäftigtendatenschutz und Compliance § 5 Rn. 10 ff.
[148] BAG Urteil vom 11.12.2014 – 8 AZR 1010/13
[149] § 26 Abs. 2 S. 2 BDSG n.F., § 49 Abs. 3 S. 2 DSG-EKD;
[150] BT-Drs. 18/11325, S. 97
[151] Dies nimmt den Rechtsgedanken des § 23 Abs. 1 Nr. 3 KUG auf, der die Abbildung von Versammlungen erlaubt hat. Dadurch wird jedoch kein Erlaubnistatbestand geschaffen, sondern nur die Freiwilligkeit der trotzdem erforderlichen Einwilligung vermutet.
[152] So aber Seifert in Simitis Datenschutzrecht Artikel 88 Rn. 218
[153] Wybitull NZA 2017, S. 413, 416
[154] Thüsing /Schmidt in Heidelberger Kommentar DS-GVO / BDSG Art. 88 Rn. 34
[155] BT-Drs. 18/11325, S. 97

eines Arbeitsvertrages oder im Zusammenhang mit anderen Leistungen wird regelmäßig die Freiwilligkeit wegen Verstoß gegen das Kopplungsverbot gem. Art 7 Abs. 4 DSGVO (§ 8 Abs. 7 KDG; § 11 Abs. 4 DSG-EKD) nach § 134 BGB unwirksam machen.[156]

Eine weitere Voraussetzung ist der Hinweis auf die Bedeutung der Einwilligung und auf den Zweck der Datenverarbeitung.[157]Im Fall der Veröffentlichung von Fotos der Beschäftigten ist die Einstellung ins Internet problematisch, weil die Betroffenen regelmäßig nicht mehr über ihre Daten verfügen können. Auch wenn eine etwaige Einwilligung widerrufen würde, könnte der Arbeitgeber die Daten zwar auf seiner Homepage löschen, die Daten blieben jedoch auf Dauer im Internet, weil Suchmaschinen darauf verlinken und diese Bilddaten jederzeit weltweit verknüpft und verwertet werden können. Auf dieses Risiko ist immer ausdrücklich hinzuweisen.[158]

Die Einwilligung ist schriftlich zu erteilen. Während nach § 4a Abs.1 S. 3 BDSG a.F. jede Einwilligung der Schriftform bedurfte, verlangt Art. 7 Abs. 1 DSGVO (§ 11 Abs. 1 DSG-EKD) nur eine Nachweispflicht. Jedoch wird in § 26 Abs. 2 S. 3 BDSG n.F. (§ 49 Abs. 3 S. 3 DSG-EKD) für das Beschäftigungsverhältnis ausdrücklich die Schriftform bestimmt.[159] Eine solche Verschärfung des Rechts an dieser Stelle hätte nicht erfolgen müssen, wenn der Gesetzgeber nicht einen besonderen Schutz der Beschäftigten hätte gewährleisten wollen. Die Behauptung *Schriftlichkeit meine nicht Schriftform i. S. d. § 126 BGB*[160] entbehrt deshalb einer Grundlage. Eine andere als die Schriftform ist nur zulässig, wenn besondere Umstände dies angemessen erscheinen lassen. Damit schreibt das Gesetz eine Ausnahmesituation fest. Ließe man eine Einwilligung in Form einer E-Mail zu, dürfte sich die Ausnahme zur Regel entwickeln und den gesetzgeberischen Willen eines besonderen Schutzes unterlaufen.[161]

Nach Art. 7 Abs. 3 DSGVO (§ 11 DSG-EKD; § 8 Abs. 6 KDG) ist der Widerruf einer Einwilligung jederzeit ohne Angaben von Gründen mit Wirkung für die Zukunft möglich. Insoweit ist die Rechtsprechung des BAG überholt, nach der es für den Widerruf eines wichtigen Grundes bedurfte. Für diese Forderung gab es im KUG zwar

[156] Seifert in Simitis Datenschutzrecht Artikel 88 Rn. 218; Schwartmann/Klein in Heidelberger Kommentar DS-GVO / BDSG Art. 7 Rn. 45; so auch Erwägungsgrund 43 zur DSGVO
[157] Erwägungsgrund 42 zur DSGVO
[158]37 TB LbfD Bremen 12.1.2
[159] Für den Anwendungsbereich des KDG ist eine spezielle Regelung nicht erforderlich, weil nach § 8 Abs. 2 weiterhin jede Einwilligung der Schriftform bedarf.
[160] So Thüsing/Schmidt in Heidelberger Kommentar DS-GVO / BDSG Art. 88 Rn. 36
[161] So im Ergebnis auch Seifert in Simitis Datenschutzrecht Art. 88 Rn. 219

keine gesetzliche Regelung, sie war jedoch allgemein anerkannt.[162] Unter der Geltung der aktuellen Datenschutzgesetze kann diese Ansicht nicht weiter aufrechterhalten werden, weil ein Rückgriff auf das KUG nicht mehr zulässig ist. Wer Fotos auf der Grundlage einer Einwilligung zunächst rechtmäßig veröffentlicht, muss also dennoch damit rechnen, dass der Abgebildete seine diesbezügliche Einwilligung widerruft und die Abbildung für die Zukunft unzulässig macht.

6.2.2.4. Ergebnis

Ein Arbeitgeber darf Bilder seiner Beschäftigten nach den Regelungen der neuen Datenschutzgesetze nur mit Einwilligung der Betroffenen verbreiten, etwa in Broschüren oder dem Internet und dem Intranet. Diese Rechtslage bestand insoweit bereits bei Geltung des BDSG a.F. und des Kunsturhebergesetzes.[163]

6.2.3. Urheberrechtsschutz bei Fotos

Einen weiteren Problembereich im Minenfeld der Fotorechte stellt das Urheberrecht dar.

Wer ein Foto erstellt, ist Urheber. Dies kann jede natürliche Person sein. Erforderlich ist weder Volljährigkeit noch Geschäftsfähigkeit. Somit können auch Kinder Urheber sein.

Der Urheberschutz beginnt mit der Herstellung des Fotos. Eine Eintragung in ein Urheberverzeichnis ist ebenso wenig erforderlich, wie das Versehen des Werkes mit einem Copyrightvermerk, der dem deutschen Recht fremd ist.

Das Urheberrecht bleibt stets bei dem Urheber. Es ist vererblich und endet erst 10 Jahre nach dem Tod des Urhebers.

Der Urheber kann also sein Urheberrecht nicht übertragen, aber Dritten ein Nutzungsrecht an seinem Werk gestatten. Dies kann entgeltlich oder unentgeltlich geschehen.

Außerdem kann der Urheber entscheiden, ob er Dritten das ausschließliche oder das einfache Nutzungsrecht übertragen möchte.

Bei der Übertragung des ausschließlichen Nutzungsrechts ist nur noch der Nutzer berechtigt, das Werk zu nutzen. Er darf dies umfassend ausüben. Selbst der Urheber ist in einem solchen Fall nicht mehr nutzungsberechtigt.

[162]OLG Frankfurt Urteil vom 24.02. 2011 - 16 U 172/10; OLG München Urteil vom 17.03.1991 - 21 U 4729/88; LG Köln Urteil vom 20.12.1995 - 28 O 406/95

[163] 3. TB TLfDI S. 314, mit Verweis auf Auernhammer / Forst Kommentar zum BDSG § 32 Rn. 68

Im Fall der Übertragung des einfachen Nutzungsrechts darf der Nutzer das Werk nur für den festgelegten Zweck nutzen.

Ist aus einer Übertragung nicht genau zu ersehen, in welchem Umfang das Nutzungsrecht übertragen worden ist, muss die Auslegung zugunsten des Urhebers ausfallen.

In jedem Fall kann das Nutzungsrecht nur mit Zustimmung des Urhebers weiterübertragen werden.

Wer also Fotos durch einen Fotografen anfertigen lässt, muss vorher die Zwecke, für die diese Fotos angefertigt werden, eindeutig festlegen. Ohne eine eindeutige Regelung steht dem Fotografen das ausschließliche Recht zu, seine Bilder zu verwerten. Demgegenüber hat die Person, die auf einem Foto abgebildet ist, kein dem Urheber vergleichbares Recht. Der Abgebildete hat also nicht das Recht, das Foto zu einem anderen Zweck zu verwenden als zu dem, zu dem es erstellt worden ist. Beispiel: Jemand verwendet Bewerbungsfotos zur Veröffentlichung auf seiner Homepage.

Zwei Fälle waren in diesem Zusammenhang von unserer Dienststelle zu bescheiden.

Bei einer Freizeitveranstaltung zum Thema „Licht“ wird einem achtjährigen Kind von der Leiterin deren Fotoapparat überlassen. Tatsächlich gelingt dem Kind eine gute Aufnahme einer Lichtinstallation, die vom Veranstalter veröffentlicht wird. Die Eltern des Kindes machen das Urheberrecht für ihr Kind geltend.

Die Überlassung des Werkzeuges (Fotoapparat) verhindert ebenso wenig wie das Alter des Kindes das Entstehen der Urheberschaft. Die Eltern können als die Sorgeberechtigten die Rechte ihres Kindes geltend machen.

In einer Pfarrei werden Bilder der ehemaligen Pfarrer in einer Galerie ausgestellt. Eines Tages wird eines der Bilder mit einem kurzen Begleittext im Pfarrbrief, der auch im Internet einzusehen ist, veröffentlicht. Der Fotograf macht gegenüber der Pfarrei sein Urheberrecht geltend und verlangt ein Honorar für die Veröffentlichung des Fotos in Pfarrbrief und Internet.

Auch wenn der Pfarrer der Veröffentlichung zugestimmt hat, berechtigt dies nicht zur Einschränkung des Urheberrechts. Wenn der Urheber (wie in diesem Fall von ihm behauptet) das Bild nur zur Ausstellung in der Galerie zur Verfügung gestellt hat, ist lediglich ein eingeschränktes Nutzungsrecht übertragen worden. Für eine Veröffentlichung im Pfarrbrief fehlt dann eine Vereinbarung. Behauptet die Pfarrei ihr sei ein weitergehendes Nutzungsrecht übertragen worden, ist sie dafür beweispflichtig.

6.3. Avatar

Problemstellung:

In einer Schule wird ein Kind unterrichtet, welches an Chronischer Erschöpfungskrankheit leidet. Hauptsymptom dieser Krankheit ist eine starke, alle Aktivitäten beeinträchtigende Müdigkeit und Erschöpfung, vor allem nach körperlichen aber auch intellektuellen Belastungen.

Die Krankheit führt dazu, dass eine geregelte, d.h. verlässlich regelmäßige Unterrichtung des Kindes in der Schule nicht möglich ist. Das Kind muss häufig aufgrund der Krankheit zu Hause, teilweise im Bett, bleiben oder auch stationär im Krankenhaus aufgenommen werden.

Um dem Kind auch in diesen Phasen eine Teilnahme am Unterricht zu ermöglichen, ist ein Avatar entwickelt worden. Dieser wird im Klassenraum aufgestellt und nimmt an Stelle des Kindes das Unterrichtsgeschehen auf. Dazu stehen ihm sowohl optische als auch akustische Aufnahmegeräte zur Verfügung.

Das Kind kann von zu Hause oder aus dem Krankenhaus, in jedem Fall also von außen, den Avatar steuern. Es kann bestimmen, ob der Avatar das Unterrichtsgeschehen filmt oder Tonaufnahmen macht, bzw. beides. Der Avatar ist insoweit beweglich, als er sich um 360° drehen kann. Ebenso ist der Kopf des Avatars in der Vertikalen schwenkbar. Auch verfügt der Avatar über Lautsprecher, über die sich das Kind am Unterricht beteiligen kann. Der Avatar zeigt durch jeweilige Lichtsignale an, in welchem Modus er sich befindet bzw. gibt durch ein Lichtsignal zu erkennen, dass das Kind sich am Unterricht beteiligen möchte. Durch die angebrachten Signallampen ist also für die anderen Schüler und das Lehrpersonal zu erkennen, ob der Avatar aktiv ist.

Die Verbindung zwischen dem Avatar und dem Endgerät des Kindes wird über das Internet hergestellt. Dabei soll ausschließlich ein Streaming in Echtzeit möglich sein. Die Verbindung ist verschlüsselt. Eine Speicherung im Sinne einer dauerhaften Aufzeichnung, die ein Abspielen der Aufnahmen zu einer anderen (späteren) Zeit erlaubt, soll bei diesem Verfahren nicht möglich sein, da entsprechende implementierte Software dies verhindert.

Die eingebundenen Server speichern nach Herstellerangaben nur Metadaten. Deren Umfang ist derzeit nicht bekannt.

Datenschutzrechtliche Stellungnahme:

Vor dem oben dargestellten Setting wird der Einsatz eines solchen Avatars durch die Datenschutzaufsicht als unzulässig betrachtet.

Dies wird durch folgende Probleme begründet:

1. Alle Schüler der betreffenden Klasse würden videoüberwacht. Diese Überwachung kann permanent stattfinden oder punktuell. Es ist nicht gesichert, dass sich jeder Schüler sicher sein kann, ob er in einem bestimmten Moment überwacht wird oder nicht, da er die entsprechenden Signallampen des Avatares nicht permanent im Blick haben wird.
2. Gleiches gilt für Tonaufnahmen des nicht öffentlich gesprochenen Wortes. Da sich die Wortbeiträge der am Unterricht Beteiligten an einen abgeschlossenen Personenkreis richten, sind diese Beiträge nicht öffentlich.
3. Eine Einwilligung der Betroffenen könnte nur generell im Vorfeld erfolgen. Dies widerspricht dem Grundsatz, dass Einwilligungen konkret zu erfolgen haben.
   Der Einwilligende weiß bei der Einwilligung nicht, welchem Personenkreis seine Daten zur Verfügung gestellt werden. (siehe 4.)
4. Es kann nicht sichergestellt werden, dass die Aufnahmen am Endgerät nur von dem kranken Schüler betrachtet werden. Auch, wenn systemseitig gewährleistet ist, dass das Streaming nur auf einem bestimmten Endgerät verfolgt werden kann, ist nicht sichergestellt, dass dieses Gerät nicht von verschiedenen Benutzern verwendet wird. Ebenfalls ist nicht gesichert, dass neben dem kranken Kind nicht auch andere Personen den Videostream verfolgen.
   Auch kann nicht ausgeschlossen werden, dass die gestreamten Aufnahmen vom Bildschirm des Endgerätes abgefilmt werden, bzw. dass Tonaufnahmen von externen Geräten aufgezeichnet werden.

Unabhängig von der technischen Ausgestaltung und Sicherung einer Datenübertragung bestehen datenschutzrechtliche Probleme also bei der praktischen Anwendung. Die damit verbundenen Einschränkungen des Rechts auf informationelle Selbstbestimmung und die Eingriffe in die Privatsphäre der anderen Beteiligten sind von derartiger Erheblichkeit, dass eine Genehmigung ausscheidet.

6.4. Unverschlüsselte E-Mailversendung personenbezogener Daten

Bei Versendung einer E-Mail ist nicht sichergestellt, dass Dritte vom Inhalt der E-Mail keine Kenntnis erhalten. Regelmäßig durchläuft eine E-Mail auf ihrem Weg vom Versender zum Empfänger zahlreiche Schnittstellen oder Server. An jeder dieser Schnittstellen ist ein Auslesen der in der E-Mail enthaltenen Daten grundsätzlich möglich.
Unbefugte können die übermittelten Informationen zur Kenntnis nehmen und manipulieren, ohne dass Absender und Empfänger der E-Mail dies bemerken. Eine unverschlüsselte E-Mail ist also offener als eine mit Bleistift geschriebene Postkarte. Genau wie bei der Postkarte sind dafür auch keine fundierten Computer- oder „Hacker"-Kenntnisse notwendig. Bereits einfache Software-Werkzeuge zur Netzwerküberwachung erlauben das Mitlesen der Nachrichten im Klartext.

Sollen personenbezogene Daten per E-Mail versendet werden, ist dies nur zulässig, wenn ein Verschlüsselungssystem verwendet wird.

6.5. Herausgabe des Pflegeberichtes für die verstorbene Mutter

Eine Petentin wandte sich an unsere Dienststelle. Sie begehrte die Herausgabe des Pflegeberichtes ihrer verstorbenen Mutter von dem Krankenhaus, in dem die Mutter zuletzt behandelt worden ist. Das Krankenhaus verweigerte die Herausgabe des Berichtes, weil es der Tochter einen Anspruch auf Herausgabe absprach. Dies allerdings ohne nähere rechtliche Begründung.
Das Einsichtnahmerecht in die Patientenakten 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 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.[164]

Nach kurzer Darstellung der Rechtslage konnte dem Krankenhaus vermittelt werden, dass ein Anspruch der Tochter auf Herausgabe der Patientenakte durchaus bestand. Das Krankenhaus teilte unserer Dienststelle daraufhin mit, dass es die Herausgabepflicht akzeptiere und sandte uns zum Beweis das Schreiben zu, welches das Krankenhaus an die Petentin geschrieben hat. Allerdings befand sich bei diesem Schreiben an uns auch der Pflegebericht der verstorbenen Mutter. Aufgrund dieses erheblichen Datenschutzverstoßes wurde ein Vor-Ort-Termin in dem Krankenhaus abgehalten. Da bei diesem Treffen von dem Krankenhaus der Fehler bereits bemerkt worden war und zwischenzeitlich umfangreiche Veränderungen im Hinblick auf die datenschutzrechtliche Situation getroffen worden sind, wie z. B. die Aktualisierung des Datenschutzkonzeptes und der Austausch des Datenschutzbeauftragten (nachdem der bis dahin zuständige Betriebliche Datenschutzbeauftragte sein Amt

[164]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

niedergelegt hatte), wurde eine förmliche Beanstandung ausgesprochen. Da zu diesem Zeitpunkt das KDG noch nicht in Kraft getreten war, stand die Verhängung einer Geldstrafe nicht zur Diskussion, da eine solche in der bis dahin geltenden KDO nicht vorgesehen war.

7. Pfarrbriefe

7.1. Verteilung

Immer wieder gibt es Anfragen, die sich mit dem Vertrieb von Pfarrbriefen oder Gemeindemitteilungen beschäftigen.

Wenn Pfarrbriefe ausschließlich Informationen zu Gottesdienstzeiten und Veranstaltungen enthalten oder weitere Texte, die keine personenbezogenen Daten enthalten, ist das Auslegen solcher Briefe in der Kirche zur Mitnahme durch Gemeindemitglieder oder Besucher unproblematisch.

Anders ist es dann, wenn Pfarrbriefe zur Mitnahme durch Verteiler in der Kirche ausgelegt werden und mit Adressaufklebern versehen sind oder die Liste derer, an die die Briefe verteilt werden sollen, den einzelnen Stapeln beigefügt ist, so dass jedermann einsehen kann, wer einen solchen Brief erhält. In beiden Fällen wird neben den Kontaktdaten der Empfänger auch das personenbezogene Datum „ist Mitglied der katholischen Kirche“ übermittelt, da üblicherweise diese Pfarreimitteilungen nur an Mitglieder verteilt werden. Fehlen auf den Listen hingegen Namen, die früher einmal zum Kreis der Empfänger gehört haben, ist das personenbezogene Datum „ist nicht mehr Mitglied“ bekannt gegeben. Für die Verarbeitung solcher personenbezogenen Daten besteht keine Rechtsgrundlage. Diese Verfahrensweise stellt einen Verstoß gegen datenschutzrechtliche Vorschriften dar.

Wird die Verteilung durch haupt- oder ehrenamtliche Verteiler wahrgenommen, denen eine Adressliste der Mitglieder ausgehändigt wird, an die sie die Pfarrbriefe zuzustellen haben, ist dieses Vorgehen unproblematisch, wenn die Verteiler zuvor auf das Datengeheimnis gem. § 5 KDG verpflichtet worden sind. Die Verteiler sind dabei darauf hinzuweisen, dass die Listen ausschließlich zu dem Zweck der Pfarrbriefverteilung zu verwenden sind und vor der Kenntnisnahme durch Dritte zu schützen sind.

7.2. Abdrucken der Namen von Verstorbenen einer Pfarrei im Pfarrbrief

Grundsätzlich endet der Datenschutz mit dem Tod. Die Information der Gemeinde, über den Tod eines Mitgliedes mit der Bitte für diesen zu beten, ist eine kirchliche Aufgabe. Die Mitteilung im Informationsorgan der Pfarrgemeinde über den Tod verbunden mit den Geburts- und Sterbedaten ist zulässig. Das gilt auch bei Veröffentlichung des Pfarrbriefes im Internet.

Die Menschenwürde bleibt jedoch auch nach dem Tod unantastbar. Der Verstorbenen soll auch nach seinem Tod vor schweren Verletzungen, die in den Kernbereich der Menschenwürde eingreifen, geschützt bleiben. Darunter können grobe Entstellungen des Lebensbildes, Verzerrungen der Identität oder Offenbarung besonders sensibler Umstände fallen.[165] Sollte in Pfarrbriefen also über die reine Todesmitteilung hinaus eine Würdigung des Lebens des Verstorbenen abgedruckt werden, ist dies zu berücksichtigen und ggf. zuvor mit den Angehörigen abzusprechen.

Eine spezialgesetzliche Ausprägung des allgemeinen Persönlichkeitsrechts findet sich in §§ 22 ff. KUG mit dem Recht am eigenen Bild. Dieses Recht gewährt den Hinterbliebenen bis zu zehn Jahren nach dem Tod über das Recht am Bild, also z. B. die Veröffentlichung des Bildes der Verstorbenen zu entscheiden. Wird also die Todesnachricht mit einem Bild des Verstorbenen veröffentlicht, ist zuvor die Zustimmung der Angehörigen einzuholen! Unabhängig von der Frage der weiteren Geltung des KDG sollte dieses Verfahren beibehalten werden.

8. Daten im Schematismus

8.1. Veröffentlichung von Mitarbeiterdaten im Amtsblatt / Internet und Schematismus

Bereits im ersten Tätigkeitsbericht wurde zu diesem Thema Stellung genommen.[166]

Auch unter der neuen Rechtslage ist eine Änderung der dort vertretenen Meinung nicht veranlasst. Eine solche Veröffentlichung ist zulässig, auch wenn eine diesbezügliche Einwilligung der/des Betroffenen nicht vorliegt und die Veröffentlichung der Daten zur ordnungsgemäßen Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist. Dies ist insbesondere bei Mitarbeitern/innen zu bejahen, die ein Leitungsamt innehaben oder ein Amt mit

[165] MüKo/Rixecker, BGB, 6. Aufl., § 12 Anh. Rn. 38
[166] 1. TB 2016 S. 14

Außenwirkung. Solche Amtsträger, zu denen auch die Mitarbeiter einer Kirchenverwaltung gehören, können sich dann und soweit nicht auf das Recht der informationellen Selbstbestimmung berufen, soweit sie als für die Kirche handelnde Personen im Rahmen einer nach außen gerichteter Aufgabe tätig werden.

Angaben, die im Zusammenhang mit einer nach außen gerichteten Tätigkeit als Amtsträger stehen, sind Name, Funktion sowie dienstliche Erreichbarkeit und Dienstort. Diese Daten können ohne Einwilligung des/der Betroffenen oder eine weitere Rechtsgrundlage an Dritte übermittelt werden.

Dies gilt im Umkehrschluss nicht für solche Mitarbeiter, die lediglich innere Dienste versehen, wie Pförtner, Buchhalter u.ä.

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

Beispiel:

Die Angabe, ein Pfarrer sei von seinem Dienst entpflichtet worden darf im Amtsblatt veröffentlicht werden.

Pfarrer XY wird vom Dienst in der Kirchengemeinde A entpflichtet und ab .... in der Kirchengemeinde B eingesetzt.

Derartige Bekanntgaben sind zulässig und auch erforderlich, da sie Auskunft über die Person als Amtsinhaber geben.

Der Grund der Entpflichtung jedoch darf in der Regel nicht mitgeteilt werden, da damit weitere persönliche Daten bekannt gegeben werden.

Z. B. …wird aus gesundheitlichen Gründen entpflichtet und aus gesundheitlichen Gründen in den Ruhestand versetzt.

Für die Bekanntgabe derartiger persönlicher Daten bedarf es einer Einwilligung des/der Betroffenen.

8.2. Adressenübermittlung an kirchliche Publikationsorgane

In der Meldestelle eines Ordinariates traf die folgende Bitte eines kircheneigenen Verlages ein: „Wir möchten wieder einmal neue Abonnenten im Bistum XY gewinnen und erbitten die Bereitstellung der Adressen der katholischen Haushaltsvorstände – möglichst recht bald. Wann wäre es Ihnen möglich, die Daten für mich in einer Excel- oder csv-Datei zusammen- und bereitzustellen? Wir würden gern Mitte März starten, müssen aber vorab noch mit den aktuellen Abonnenten abgleichen.“

Leider gibt es immer wieder Differenzen mit den Kirchenzeitungen im Hinblick auf die Herausgabe von Meldedaten, die von den Verlagen zur Werbung für die von ihnen herausgegebenen Printmedien verwendet werden sollen. Bereits im ersten Tätigkeitsbericht ist auf diesen Missstand hingewiesen worden.

Bereits im Jahr 2016 wurde gegenüber den Bistümern sowie dem Verlag eine förmliche Beanstandung ausgesprochen. Damals stellte sich heraus, dass der Verlag die vom Bistum erhaltenen Meldedaten an ein Unternehmen der Deutschen Telekom weitergab, um zu den Meldedaten die Telefonnummern heraussuchen zu lassen. Die so ermittelten Telefonnummern wurden dann zu Werbezwecken angerufen. Dieses Verfahren stellt in mehrfacher Hinsicht einen groben Verstoß gegen datenschutzrechtliche Bestimmungen dar und widerspricht außerdem dem Gesetz gegen unlauteren Wettbewerb. Es wurde damals ausdrücklich darauf hingewiesen, dass telefonische Werbung in jedem Fall, ebenso wie E-Mailwerbung ohne Einverständnis, unzulässig ist.

Weiterhin wurde in der seinerzeitigen Beanstandung aber auch auf einen Weg aufgezeigt, wie durch den jeweiligen Ortsbischof in Einbindung mit dem Verlag eine rechtskonforme Werbung für das Printmedium möglich ist. Dies kann im Wege der Auftragsdatenverarbeitung geschehen. Das Verfahren wurde den Beteiligten ausführlich dargestellt.

Bedauerlicher Weise gehört der hier angesprochene Verlag zu den unter Punkt 1.3. angesprochen Einrichtungen, die sich dem KDG nicht verpflichtet sehen, sondern auf seiner Homepage in der Datenschutzerklärung die Anwendbarkeit der staatlichen Regelungen der DSGVO für sich propagiert.

Es erscheint dringend erforderlich, den Verlag zu verpflichten, derartige Anforderungen gegenüber den kirchlichen Stellen zu unterlassen und sich eindeutig und ausdrücklich dem KDG zu unterstellen.

10. Videoüberwachung in Schulen

Die in § 52 KDG geregelte Zulässigkeit von Videoüberwachungen erlaubt in bestimmten Grenzen nur die Videoüberwachung öffentlich zugänglicher Räume (§ 52 Abs. 1 KDG).

Öffentlich zugänglich sind solche Räume, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten oder benutzt werden können[167].

[167] Bergmann/Möhrle/Herb, Kommentar zum BDSG aF § 6b Rn. 22; Scholz in Simitis/Hornung/Spiecker Datenschutzrecht Anhang 1 zu Art. 6 Rn. 56

Dazu gehören Schulgebäude, soweit es den allgemein zugänglichen Teil betrifft sowie deren öffentlich zugängliche Außenanalgen.

Demgegenüber sind nicht-öffentliche Räume solche, die nur von einem bestimmten oder genau abgegrenzten Personenkreis betreten werden dürfen.[168] Dazu zählen z.B. Klassen- oder Kursräume.

Gem. § 52 Abs. 1 lit. a KDG ist eine Videobeobachtung zulässig, wenn sie zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder nach § 52 Abs. 1 lit. b KDG zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist.

In der Regel wird es nicht zur Aufgabenerfüllung einer Schule gehören, allgemeine Videoaufnahmen von Schülern und Besuchern zu erstellen. Etwas anderes mag für Videoaufnahmen im Rahmen von Projekten, wie Kunst- oder Theaterprojekten, gelten. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer das Gebäude betreten und sich darin aufhalten darf[169].

Dies rechtfertigt es, eine Videoanlage im Monitoring-System zu installieren, wenn die übrigen Voraussetzungen gegeben sind. Eine solche Anlage z. B. im Eingangsbereich ist dann zulässig, wenn dieser sonst nicht einsehbar ist. Erforderlich ist stets die direkte Überwachung mit sofortiger Eingriffsmöglichkeit.

Der Eingriff in das Persönlichkeitsrecht der betroffenen Besucher, bzw. Schüler ist in einem solchen Fall gering. Da durch die Videoanlage an dieser Stelle keine Aufzeichnung erfolgt und auch biometrische Auswertungen nicht stattfinden, ist die Eingriffstiefe nicht höher, als wenn die Betroffenen an einem Fenster vorbeigingen.

§ 52 Abs. 1 lit.b:

Die Wahrnehmung berechtigter Interessen setzt das Bestehen einer konkreten Gefährdungslage voraus. Hierfür sind konkrete Vorfälle darzulegen, die eine Anbringung der Videoüberwachung gerade an dieser Stelle erforderlich machen. Eine bloße Behauptung oder Vermutung, dass Rechtsverletzungen gerade an dieser Stelle zu erwarten sind, reicht nicht aus[170].

Weiterhin müsste eine konkrete Zweckbestimmung vorliegen, d. h. das konkrete Ziel der Überwachung müsste benannt sein. Allgemeine Erklärungen wie *„Gefahr von Diebstählen oder Sachbeschädigungen*“ werden dem nicht gerecht[171].

In der Regel lassen sich durch eine Videoüberwachung im Aufzeichnungssystem Straftaten nicht verhindern. In diesen Fällen soll die Überwachung lediglich der

[168] Scholz in Simitis Kommentar zum BDSG § 6b Rn. 48; ders. in Simitis/Hornung/Spiecker Datenschutzrecht Anhang 1 zu Art. 6 Rn. 59
[169] Scholz in Simitis Kommentar zum BDSG § 6b Rn. 73
[170] BGH NJW 1995, 1950 (1957); Scholz in Simitis Kommentar zum BDSG § 6b Rn. 80
[171] So auch BfDI 23. Tätigkeitsbericht Pkt. 12.1. (dort zum Thema Beschäftigtendatenschutz)

Verfolgung des Straftäters dienen und vermittelt bestenfalls ein subjektives Sicherheitsempfinden. Objektiv führen Videoaufzeichnungen häufig nicht dazu, Straftaten zu vermeiden[172]. Dadurch, dass Täter häufig ihr Gesicht bedecken, sind auch für die Strafverfolgung die Aufnahmen nur bedingt geeignet. Schließlich müsste der Täter direkt bei Begehung der Straftat gefilmt werden. Allein der Nachweis, dass eine bestimmte Person sich zu einer Zeit an einem Ort aufgehalten hat, an dem dort auch eine Straftat begangen worden ist, wird regelmäßig nicht ausreichen, um zu einer Verurteilung zu führten. Bei einer nur abstrakten Gefährdung fehlt das berechtigte Interesse[173].

Vor der Inbetriebnahme ist also darzulegen, ob bereits Straftaten der benannten Art, also Diebstähle oder Sachbeschädigungen von oder an Eigentum des Verantwortlichen oder Dritten stattgefunden haben.

Weiterhin ist der konkrete Zweck ausdrücklich zu benennen und auszuschließen, dass die Aufzeichnungen für andere als durch den Zweck vorgegebene Maßnahmen genutzt werden (z. B. zu Sanktionierung von Verunreinigungen oder Rauchern).

Kameras im nicht öffentlichen Bereich

Macht der Verantwortliche deutlich, dass er den Zugang zu Räumen nicht mehr gestattet, stellen diese Räume keine öffentlichen Räume mehr dar. Dabei kommt es nicht darauf an, ob es eine faktische Zugangsmöglichkeit, z. B. das Betreten durch eine nicht verschlossene Tür gibt. Ein solcher Zugang, der zwar möglich ist, sich aber gegen den erkennbaren Willen des Verfügungsberechtigten richtet, stellt keine Öffentlichkeit der Räume dar.[174]

Werden Kameras außerhalb des Schulbetriebs aktiviert, wenn das Schulgelände geschlossen ist, kann die Zulässigkeit nicht nach § 52 KDG beurteilt werden.

Da § 52 KDG nur die Videoüberwachung in öffentlich zugänglichen Räumen regelt, muss die Videoüberwachung für andere Räume nach den allgemeinen Vorschriften beurteilt werden.

Es handelt sich bei Bildern, die durch optische Geräte aufgenommen werden, um personenbezogene Daten. Deren Verarbeitung ist u.a. rechtmäßig, wenn die Voraussetzungen des § 6 Abs. 1 lit g) gegeben sind. Auch nach dieser Vorschrift ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn es berechtigte Interessen des Verantwortlichen oder Dritter zu wahren gilt. Das berechtigte Interesse

[172] Datenschutznachrichten Heft 3 2010, Seite 121. Zu den Ergebnissen einer Videoüberwachung in Hamburg bei der festgestellt worden ist, dass die Zahl der Straftaten trotz intensiver Videoüberwachung gestiegen ist.
[173] Scholz in Simitis/Hornung/Spiecker Datenschutzrecht Anhang 1 zu Art. 6 Rn. 77
[174] Wedde in DKWW § 6 b Rn. 20

ist weit auszulegen.[175] Damit dürfte der Zweck der Sicherung gegen Fremdnutzung des überwachten Raumes darunterfallen. Insbesondere wenn es um Verkehrssicherungspflichten des Verantwortlichen geht und darum diesen Raum nicht zum Umschlagplatz von Waren werden zu lassen, deren Vertrieb rechtswidrig ist. Weiterhin ist die Sicherung des Eigentums, insbesondere gegen Diebstahl und Einbruchdiebstahl in ansonsten schwer einsehbaren Teilen des Geländes, als berechtigtes Interesse anzuerkennen.

Weiterhin müsste die Videoüberwachung zur Erreichung des Zwecks erforderlich sein. Soweit der Zweck in der Verhinderung der genannten Taten besteht, erscheint es zweifelhaft, ob die Videoüberwachung dazu geeignet ist. Im Hinblick auf eine Strafverfolgung wird dies regelmäßig nicht der Fall sein, s. o. Allerdings kann davon ausgegangen werden, dass eine offene Videoüberwachung, auf die durch entsprechende Piktogramme und Informationen hingewiesen wird, abschreckend insbesondere auf Personen wirkt, die den überwachten Teil zum versteckten Handel nutzen möchten. Zur Erreichung dieses Zwecks wäre die Verwendung von Videotechnik auch erforderlich, da auf andere Weise der gleiche Zweck nicht erreicht werden kann. Dies träfe insbesondere zu, wenn man eine erhöhte Kontrolle durch Personal als ein milderes Mittel fordern wollte. Derartige Maßnahmen sind in der Regel nicht geeignet, unerlaubte Handlungen der geschilderten Art zu verhindern.

Weiterhin müsste die Videoüberwachung verhältnismäßig sein. Da sich nach Beendigung des Schulbetriebes, wenn die Kameras aktiviert werden, in dem erfassten Bereich keine berechtigen Personen mehr aufhalten sollen, steht eine Beeinträchtigung von berechtigten Interessen betroffener Personen nicht entgegen.

Zu berücksichtigen ist, dass die Aufzeichnungen nur zeitlich eingeschränkt verwendet werden dürfen. Es ist zu gewährleisten, dass diese Daten spätestens nach 72 Stunden gelöscht werden, sofern es sich nicht um Aufzeichnungen handelt, die zur Strafverfolgung erforderlich sind.

Weiterhin ist durch die Anlagen zu berücksichtigen, dass Bereiche, die nicht zu den Räumen des Verantwortlichen gehören, ausgeblendet werden und somit solche Räume nicht von der Überwachung erfasst werden.

[175] Frenzel in Paal/Pauly Art. 6 Rn. 28

Herausgeber:

Diözesandatenschutzbeauftragter
der ostdeutschen Bistümer und
des Katholischen Militärbischofs

Margaretenstraße 1
39218 Schönebeck
Tel.: 03928 / 7287181

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