## Gliederung

# D 1 Datenschutz

## 1. Einleitung

Die katholische Kirche hatte bislang eine eigene kirchliche Datenschutzordnung, (KDO), welche teilweise in Abweichung zum bisherigen Bundesdatenschutzgesetz (BDSG - alte Fassung) Regelungen zum kirchlichen Datenschutz getroffen hat. Die Ermächtigung für diese Ausnahmeregelung wurde aus dem in Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV verankerten kirchlichen Selbstbestimmungsrecht abgeleitet.

Europarecht hatte praktisch für den kirchlichen Datenschutz in Deutschland keine Rolle gespielt, da die Europäische Union (EU) das Thema Datenschutz nur in der EU-Datenschutzrichtlinie (RL 95/46/EG) geregelt hat. Richtlinien der EU entfalten aber keine unmittelbare Wirkung auf staatliches (deutsches) Recht. Vielmehr müssen diese durch die jeweiligen EU-Mitgliedsstaaten erst in nationales Recht umgewandelt werden. Dies erfolgte in Deutschland durch das BDSG (alte Fassung).

Im Jahr 2016 hat die EU entschieden, das Thema Datenschutz in der Verordnung EU 2016/679, der **Datenschutz-Grundverordnung (DSGVO)** zu regeln, die seit dem 25.5.2018 zur Anwendung kommt. Im Unterschied zu einer Richtlinie muss eine Verordnung nicht mehr in nationales Recht umgesetzt werden, sondern **gilt unmittelbar in jedem EU-Mitgliedsstaat.** Mitgliedsstaaten dürfen somit nur noch ergänzende Regelungen zum Datenschutz erlassen, soweit die DSGVO eine solche Ausnahme zulässt. Von dieser Regelungskompetenz hat Deutschland Gebrauch gemacht, indem es das Bundesdatenschutzgesetz (BDSG) mit Wirkung ab dem 25.5.2018 angepasst hat (BDSG-neue Fassung).

Durch diese unmittelbare Wirkung der DSGVO entfällt zunächst auch die bisher aus dem in Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV verankerten kirchlichen Selbstbestimmungsrecht abgeleitete Ermächtigung zur Schaffung eines eigenen kirchlichen Datenschutzes. Allerdings hat die EU den Kirchen in Art. 91 DS-GVO eine Regelungskompetenz zugestanden. Diese Vorschrift hat folgenden Wortlaut:

**Art. 91 DSGVO**

**Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften**

*(1) Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.*

*(2) Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht*

*durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt."*

30 In den Erwägungsgründen zur DSGVO wurde festgehalten, dass durch diese **Öffnungsklausel** die Kirchen in ihrer Rolle nicht beeinträchtigt werden sollen. Dort heißt es:

35 **Erwägungsgrund 165:**

**Keine Beeinträchtigung des Status der Kirchen und religiösen Vereinigungen**

*Im Einklang mit Artikel 17 AEUV achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren bestehenden verfassungsrechtlichen Vorschriften genießen, und beeinträchtigt ihn nicht.*

40 **In Art. 17 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) heißt es:**

*(1) Die Union achtet den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, und beeinträchtigt ihn nicht.*

*(2) Die Union achtet in gleicher Weise den Status, den weltanschauliche Gemeinschaften nach den einzelstaatlichen Rechtsvorschriften genießen.*

*(3) Die Union pflegt mit diesen Kirchen und Gemeinschaften in Anerkennung ihrer Identität und ihres besonderen Beitrags einen offenen, transparenten und regelmäßigen Dialog.*

45 **Fazit:** Die katholische Kirche ist also berechtigt, sich nach Maßgabe des Art. 91 DSGVO eigene Regelungen zum Datenschutz zu geben. Dies wurde durch die Schaffung des kirchlichen Datenschutzgesetzes (KDG), welches am 24.5.2018 die kirchliche Datenschutzordnung (KDO) abgelöst hat, versucht umzusetzen.

50 Zunächst sollen Inhalt und Umfang dieser Ermächtigung dargestellt werden.

## 1.1 Kirche, religiöse Vereinigung oder Gemeinschaft

55 Die Ausnahmeregelung in Art. 91 DSGVO dient unter Bezugnahme auf den Erwägungsgrund 165 der DSGVO der Umsetzung von Art. 17 AEUV. Zunächst ist also für die Anwendbarkeit dieser Ausnahmeregelung erforderlich, dass eine staatliche Regelung besteht, welche der Kirche besondere Kompetenzen zuweist[1].

60 Es geht darum, Kirchen sowie religiöse Vereinigungen oder Gemeinschaften, welche nach staatlichem Recht besondere Regelungskompetenzen

1 Ehmann/Selmayr, Art. 91 DS-GVO, Rn 1 ff.

erhalten haben, zu schützen. In Deutschland wurde durch Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV der katholischen Kirche ein solches Selbstbestimmungsrecht zugestanden.

Nur unter diesem Aspekt enthält Art. 91 DSGVO eine begrenzte Bereichsausnahme vom Unionsrecht. **Eine generelle Bereichsausnahme für religionsrelevante Sachverhalte begründet er dagegen nicht.** Vielmehr besteht die Regelungskompetenz der Kirchen nur im Rahmen der in Art. 91 DSGVO aufgestellten Kriterien und bleibt nach der hier vertretenen Ansicht hinter der bisherigen Ermächtigung im Verhältnis zum rein deutschen Recht des BDSG (alte Fassung) zurück. 65

Allerdings ist nach dem Wortlaut des Art. 91 DSGVO kein Zusammenhang der Datenverarbeitung mit der spezifisch religiösen Aufgabe erforderlich. Das bedeutet, dass sich Ausnahmeregelungen der Kirche nicht nur auf die Daten von Mitgliedern beziehen müssen. Die Kirche ist beispielsweise auch berechtigt, **generelle Regelungen zum Mitarbeiterdatenschutz** zu erlassen, sogar wenn es um Daten von Nichtmitgliedern der katholischen Kirche geht[1]. 70

## 1.2 Umfassende eigene Datenschutzregeln

Eine weitere Voraussetzung für die Anwendbarkeit der Ausnahmeregelung des Art. 91 DSGVO ist, dass die Kirche „umfassende“ eigene Datenschutzregelungen trifft. Hier ist in der Literatur umstritten, was darunter zu verstehen ist: 75

- Die eine Rechtsansicht vertritt die Meinung, dass unter umfassenden Regelungen nur ein im Verhältnis zur DSGVO in sich geschlossenes und abschließendes Datenschutzrecht verstanden werden kann[2].
- Eine andere Rechtsansicht geht davon aus, dass es genügt, wenn einzelne Regeln des Datenschutzrechts - beispielsweise der Beschäftigtendatenschutz - im Vergleich zur DSGVO umfassend sein müssen und es nicht notwendig ist, dass ein komplettes Datenschutzrecht durch die Kirche erlassen wird[3].

**Konsequenz:** Nach der dargestellten zweiten Meinung würde bei nur lückenhafter Ausgestaltung eines kirchlichen Datenschutzrechts für nicht geregelte Teile die DSGVO gelten. Nach der ersten Ansicht wären die gesamten kirchlichen Regelungen unwirksam und es würde insgesamt die DSGVO gelten.

Zur Vermeidung dieser Unwägbarkeit hat sich die katholische Kirche entschieden, im KDG komplett die Regelungen der DSGVO umzusetzen. 80

1 Ehmann/Selmayr, Art. 91 DS-GVO, Rn 18
2 Vgl. z.B. Ehmann/Selmayr, Art. 91 DS-GVO, Rn 17
3 Vgl. z.B. Paal/Pauly, Art. 91 DS-GVO, Rn 12 ff.

### 1.3 Anwendung zum Zeitpunkt des Inkrafttretens der DSGVO

85 Die Ausnahmeregelung des Art. 91 DSGVO ist eine **Bestandsschutzregelung**. Denn Ausnahmen für die Kirche sind danach nur erlaubt, wenn die kirchliche Regelung zum Zeitpunkt des In-Kraft-Tretens der DSGVO bereits angewendet wurde. Der **Zeitpunkt des In-Kraft-Tretens der DSGVO** ist nach Art. 99 Abs. 1 DSGVO der zwanzigste Tag nach der Veröffentlichung im Amtsblatt, also der 25.5.2016.

90 Art. 91 DSGVO gestattet es den Kirchen nicht, umfassende Datenschutzregeln erst nach dem Stichtag zu erlassen[1].

95 Im Bereich der **katholischen Kirche** wurde zum Stichtag die KDO angewendet, welche sich am BDSG in der alten Fassung orientiert hat. Erst nach dem Inkrafttreten der DSGVO ist das KDG erlassen worden. Insoweit könnte man die Ansicht vertreten, dass das KDG nicht von der Ausnahmeregelung des Art. 91 DSGVO umfasst ist und aus diesem Grund unwirksam ist. Nachdem aber in Art. 91 DSGVO auch von der kirchlichen Regelung verlangt wird, dass diese in Einklang mit der DSGVO zu bringen ist (→ Ziffer 1.4), ist der Erlass des KDG nach der hier vertretenen Ansicht grundsätzlich von der Ausnahmeregelung umfasst. Denn im Wesentlichen wurde versucht, in den kirchlichen Datenschutz die Wertungen der DSGVO zu übernehmen.

### 1.4 Das Verhältnis der Datenschutzregelungen

#### 1.4.1 Verhältnis DSGVO/BDSG

100 Bereits vor Inkrafttreten der DSGVO bestand mit der Richtlinie 95/46/EG vom 24.10.1995 eine europäische Datenschutzregelung. Eine Richtlinie im Europarecht ist ein Rechtsakt, in dem ein von allen EU-Ländern zu erreichendes Ziel festgelegt wird. Es ist jedoch Sache der einzelnen Länder, eigene Rechtsvorschriften zur Verwirklichung dieses Ziels zu erlassen.[2] Eine Verordnung ist demgegenüber ein verbindlicher Rechtsakt, den alle Mitgliedstaaten in vollem Umfang umsetzen müssen.[3]

105 Die DSGVO ist als europäische Verordnung deshalb **unmittelbar geltendes Recht** in den Mitgliedstaaten der EU. Damit kommt ihr Anwendungsvorrang vor jedem anderen nationalen Recht zu.

110 Aufgrund der unmittelbaren Geltung der Verordnung ist es dem nationalen Gesetzgeber nicht gestattet, die Vorschriften der Verordnung in

1 Kühling/Buchner, DS-GVO Art. 91, Rn 12 f.; a.A. Paal/Pauly Art. 91 DS-GVO Rn 18 f., der die Meinung vertritt, dass auch nachträglich Datenschutzregelungen von Kirchen erlassen werden können und es sich nicht nur um ein Recht auf Bestandsschutz handelt.
2 Art. 288 Satz 3 AEUV
3 Art. 288 Satz 2 AEUV

eigenen Gesetzen nochmals zu wiederholen.[1] Im Interesse einer Verständlichkeit ist lediglich die Wiederholung einzelner Punkte einer Verordnung erlaubt.[2] Dies wird auch in Erwägungsgrund 8 der DSGVO noch einmal deutlich gemacht. Danach dürfen die Nationalstaaten Teile der Verordnung in nationales Recht aufnehmen, soweit diese **für die Verständlichkeit des nationalen Rechts** erforderlich sind. Eine Abänderung der europäischen Verordnung durch den nationalen Gesetzgeber ist weder nach unten noch nach oben zulässig. Also auch eine Verschärfung der Datenschutzanforderungen im nationalen Gesetz verstieße gegen Europarecht.

Das BDSG darf daher nur solche Regelungen, für die die DSGVO nationale Regelungen zugelassen hat, neben die Regelungen der DSGVO stellen. Für den Rechtsanwender ergibt sich daraus die Verpflichtung, zunächst in der DSGVO eine Regelung zu suchen, die auf den jeweiligen Sachverhalt anwendbar ist, und soweit dort eine Öffnungsklausel enthalten ist, das BDSG zu Rate zu ziehen. 115

Das BDSG enthält in Teil 1 gemeinsame Bestimmungen. Teil 2 regelt Durchführungsbestimmungen gem. der DSGVO (also der **Verordnung**). Teil 3 betrifft die Umsetzung der **Richtlinie** (EU) 2016/680 (Datenschutzrichtlinie Polizei und Justiz). Die in Teil 3 geregelten Sachverhalte finden im nicht-öffentlichen Bereich keine Anwendung. So wäre z. B. ein Rückgriff auf die Vorschrift des § 53 BDSG ein Fehler, wenn es um die Verpflichtung auf das Datengeheimnis im nicht öffentlichen Bereich geht. 120

### 1.4.2 DSGVO/KDG

Aus den genannten Gründen wird deutlich, dass bzw. warum die Bundesrepublik nicht ein einheitliches Datenschutzgesetz erarbeiten konnte, indem die Normen der DSGVO die nationalen Regelungen gleichsam in sich aufnehmen und so ein Werk aus einem Guss entstehen lassen. Religionsgemeinschaften war dies aber möglich, weil die DSGVO für sie gem. Art. 91 überhaupt keine direkte Anwendung findet. Das KDG steht also nicht auf einer Ebene mit dem BDSG, sondern es gilt **anstelle der DSGVO.** Der Rechtsanwender muss einen Sachverhalt also nur vor den Regelungen eines Gesetzes prüfen. 125

Für die Einordnung des kirchlichen Datenschutzes ist es von Bedeutung, sich des Umfangs der Verarbeitung personenbezogener Daten in den Kirchen bewusst zu werden. Die beiden großen Kirchen in Deutschland beschäftigen ca. 1,2 Mio. Mitarbeiter. Sie verarbeiten die Daten von ca. 45 Mio. Mitgliedern[3]. Darüber hinaus werden die Daten der Besucher von 130

1 Verstoß gegen das Wiederholungsverbot: Sydow, Europäische Datenschutzgrundverordnung, 2. Auflage 2018, § 37 Rn. 140

2 EuGH, Urteil vom 28.3.1985, C-272/83

3 Quelle: www.tagesschau.de vom 2.5.2019 mit Verweis auf das „Forschungszentrum Generationenverträge“ an der Universität Freiburg

kirchlichen Kindereinrichtungen und Schulen verarbeitet. Weitere zum großen Teil sensible personenbezogene Daten verarbeiten die kirchlichen Krankenhäuser, Pflegeheime, Sozialeinrichtungen und Beratungsstellen. Damit zählen die Kirchen zu den größten Verarbeitern personenbezogener Daten in Deutschland.[1]

135 Vor diesem Hintergrund wird schnell klar, dass Kirchen keine datenschutzfreien Sektoren sein können.[2] Art. 91 DSGVO stellt deshalb auch **keine Bereichsausnahme für Religionsgemeinschaften** dar, sondern bindet diese an das Schutzniveau der DSGVO. Zulässig sind damit lediglich bereichsspezifische Regelungen, die das Schutzniveau insgesamt aber nicht absenken dürfen.[3]

140 Die Regelungen der Religionsgemeinschaften müssen gem. Art. 91 DSGVO mit der europäischen Verordnung *„in Einklang stehen"*. Diese Formulierung kann nicht so gedeutet werden, dass die kirchlichen Regelungen völlig deckungsgleich zu sein haben bzw. mit diesen völlig übereinstimmen.[4] Verstünde man Art. 91 DSGVO so, liefe dies darauf hinaus, den Religionsgemeinschaften lediglich das Abschreiben staatlicher Normen unter eigener Überschrift zu gestatten.[5] Vielmehr ist diese Vorschrift dahin zu verstehen, dass kirchliche Regelungen die Grundsätze und Wertungen der DSGVO in sich aufzunehmen haben. Dies entspricht dem Zweck des Art. 91. Mit dieser Vorschrift soll zum einen eine Harmonisierung der Datenschutzvorschriften innerhalb der Religionsgemeinschaften mit der DSGVO bewirkt werden und gleichzeitig dem verfassungsrechtlichen Status der Kirchen genüge getan werden.[6]

145 Mit einer Harmonisierung und dem Willen des Verordnungsgebers, eine kohärente Datenschutzregelung zu schaffen, besteht für die Zulassung einer Abweichung vom Schutzniveau nach unten grundsätzlich kein Raum.[7] Eine Ausnahme kann im Einzelfall dann bestehen, wenn beachtlichen Rechten der Kirche relativ leichte Beeinträchtigungen des Persönlichkeitsrechts des Betroffenen gegenüberstehen.[8] Demgegenüber gilt es überwiegend als zulässig, dass kirchliche Vorschriften einen höheren Schutzstandart festlegen dürfen.[9]

1 Seifert in Simitis, Datenschutzrecht DSGVO mit BDSG, 1. Auflage 2019, Art. 91 Rn. 7
2 Hense in Sydow, Art. 91 Rn. 11
3 Seifert in Simitis, Art. 91 Rn. 12
4 Hense in Sydow, Art. 91 Rn. 20 mit Verweis auf Ziegenhorn/Drossel, KuR 2016, 230, 241
5 Losem, KuR 2013, 231, 242
6 Thüsing/Rombey, Heidelberger Kommentar DSGVO/BDSG, 1. Auflage 2018, Art. 91 Rn. 8
7 Hense in Sydow, Art. 91 Rn. 23
8 Hense in Sydow, Art. 91 Rn. 23 am Beispiel des Löschungsrechts gem. Art 17 DSGVO gegenüber dem Recht der Kirche, Taufbucheinträge einer Löschung zu entziehen.
9 Seifert in Simitis, Art. 91 Rn. 13; Thüsing/Rombey, Art. 91 Rn. 13; Hense in Sydow, Art. 91 Rn. 21; a. A. Herbst in Kühling/Buchner, DSGVO, 2. Auflage 2018, Art. 91 Rn.15

## 1.5 Sachlicher Geltungsbereich des KDG

Der sachliche Geltungsbereich wird durch § 2 KDG bestimmt. Umfasst wird jede *„ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten"*. 150

Das KDG gilt auch für nicht automatisierte Verarbeitung personenbezogener Daten, wenn diese in einem Dateisystem gespeichert sind oder werden sollen. Ein Dateisystem ist nach der Definition des § 4 Nr. 8 KDG *„jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind …"* Damit kommt es auf die Art und Weise der Verarbeitung, manuell oder automatisiert also nicht an.[1]

Eingeschlossen von der Regelung sind weiterhin personenbezogene Daten, die noch nicht erfasst sind, aber die erhoben werden, um sie zukünftig in ein Dateisystem aufzunehmen. Dabei genügt die Aussicht, dass sie in ein Dateisystem aufgenommen werden können. Darunter fallen z. B. Informationen über einen Bewerber im Internet.[2] 155

Der Begriff des Verarbeitens umfasst gem. § 4 Nr. 3 KDG nunmehr alle Arten des Umgangs mit Daten. „Verarbeiten" umfasst nunmehr also „erheben", „verarbeiten" und „nutzen", die zuvor in § 2 Abs. 2 – 5 KDO geregelt waren. 160

Automatisiert ist eine Verarbeitung, wenn sie mit Hilfe von Informationstechnik geschieht.[3] Eine nähere Definition von Informationstechnik ist im Hinblick auf die Technikneutralität des Gesetzes nicht erfolgt. Dabei wird von dieser Regelung jede Art von Datenverarbeitungsanlage erfasst. Darunter fallen also neben Computern beispielsweise auch Tablets, PDA, Smartphone, Überwachungsanlagen wie Webcam, Dashcam, Zeiterfassungs- und Zugangssysteme, Kopierer, Scanner, Internet und E-Mail.[4] 165

**Personenbezogene Daten** sind gem. § 4 Nr. 1 KDG *„alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen"*. Danach sind nur natürliche Personen im Zeitraum von ihrer Geburt bis zum Tod von den Regelungen des Datenschutzes erfasst. Für juristische Personen gelten diese Regelungen grundsätzlich nicht. 170

Identifiziert ist eine Person dann, wenn die Person aus der Information selbst ermittelt werden kann,[5] wenn klar ist, dass sie gemeint ist.[6] Als identifizierbar ist eine Person nach § 4 Nr. 1 Satz 2 KDG insbesondere dann anzusehen, wenn sie mittels Zuordnung zu einer Kennung wie einem Na- 175

1 Erwägungsgrund 15 zur DSGVO
2 Ernst in Paal/Pauly, Datenschutzgrundverordnung 2017, Art. 2 Rn. 10
3 Roßnagel in Simitis, Art. 2 Rn. 14
4 Paal/Pauly, Art. 2 Rn. 2; Pabst in Heidelberger Kommentar, Art. 2 Rn. 27
5 Schwartmann/Mühlenbeck in Heidelberger Kommentar, Art. 4 Rn. 20
6 Ziebarth in Sydow, Art. 4 Rn. 17

men, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Auskunft der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Ist also eine Angabe einer bestimmten Person zuzuordnen, liegt ein personenbezogenes Datum auch dann vor, wenn die Person erst mithilfe von Referenzdaten ermittelt werden kann.[1] Entscheidend für das Merkmal der Identifizierbarkeit ist, dass eine vorhandene Information erst durch Hinzuziehung weiterer Informationen eine Identifizierung ermöglicht.[2]

### 1.6 Organisatorischer Geltungsbereich des KDG

180 Der organisatorische Geltungsbereich wird durch § 3 KDG bestimmt. Soweit danach in Abs. 1 lit a der verfasst-kirchliche Bereich in den Anwendungsbereich des KDG aufgenommen wird, gab und gibt es keine Differenzen darüber, ob die Kirche überhaupt berechtigt ist, ein eigenes Datenschutzrecht zu etablieren. Wie bereits dargestellt, ergab sich auch nach der alten Rechtslage das Recht der Kirchen darauf, ihre eigenen Angelegenheiten selbst zu regeln aus Art. 137 WRV, Art. 140 GG. Daraus wurde aber teilweise in der Literatur der Schluss gezogen, dass sich das Recht auf eigene Datenschutzregelungen auf Kerntätigkeiten religiöser Betätigungen zu beschränken habe („Subsumptionslösung"), also auf den Umgang mit Daten ihrer Mitglieder, Angelegenheiten der Religionsausübung, das Innehaben und Ausüben religiöser Ämter und Funktionen und dergleichen.[3] Die wohl überwiegende Meinung vertrat jedoch auch unter der alten Rechtslage die Meinung, eine Differenzierung zwischen Grundauftrag und sonstigen Aufgaben der Kirchen finde nicht statt und die Kirchen seien berechtigt, auch im Bereich ihrer privatrechtlich organisierten Einrichtungen ihre eigenen Datenschutzvorschriften anzuwenden, ohne dem BDSG zu unterliegen.[4]

185 Während des Gesetzgebungsverfahrens zur EU-Verordnung gab es eine breite Diskussion darüber, wie Datenschutz in Religionsgemeinschaften umgesetzt werden soll, von der schlichten Forderung nach Geltung der DSGVO auch für die Kirchen bis zu der Forderung, dass kirchliche Datenschutzgesetze nur einen angemessenen Schutz aufweisen müssten. Im Ergebnis soll durch Art. 91 DSGVO auch im Bereich der Kirchen ein der Verordnung adäquater Datenschutz gewährleistet werden. Gleichzeitig soll aber der verfassungsrechtlich gewährleistete Status der Kirchen erhalten bleiben. Erwägungsgrund 165 legt dies ausdrücklich mit Hinweis auf Art. 17 AEUV fest.

1 Paal/Pauly, Art. 4 Rn. 8
2 Schwartmann/Mühlenbeck in Heidelberger Kommentar, Art. 4 Rn. 25
3 Dammann in Simitis, Kommentar zum BDSG, 8. Auflage 2014, § 2 Rn. 109
4 Preuß, ZD 2015, 217, 222

Die DSGVO definiert die Begriffe „Kirche“, „religiöse Vereinigung“ und „religiöse Gemeinschaft“ nicht und kann dies auch nicht eigenständig tun, da damit unzulässig in das Staatskirchenrecht der Mitgliedstaaten eingegriffen würde.[1] Das BVerfG hat jedoch in seiner „Goch-Entscheidung“[2] den Geltungsbereich des kirchlichen Selbstbestimmungsrechts auf all jene, der Kirche zugeordneten Einrichtungen ohne Rücksicht auf deren Rechtsform erstreckt, *„wenn sie nach kirchlichem Selbstverständnis ihrem Zweck oder ihrer Aufgabe nach berufen sind, ein Stück Auftrag der Kirche in dieser Welt wahrzunehmen und zu erfüllen“*. Religionsgesellschaften können also den Begriff der Kirchlichkeit weitgehend selbstständig festlegen, was nur eingeschränkt staatlicher Kontrolle unterliegt.[3] Dies trifft in jedem Fall für die in § 3 Abs. 1 lit b KDG benannten Einrichtungen zu. Ebenfalls für die unter lit c benannten Einrichtungen. Die Grenze ist dort erreicht, wo die Einrichtung sich ausschließlich wirtschaftlich betätigt.[4] 190

Weiterhin ist es abzulehnen, Religionsgemeinschaften gemäß nationalem Recht einen Freiraum von der DSGVO zu gestatten. Soweit Regelungen der Kirchengesetze möglicherweise Wertungen der DSGVO entgegenstehen, verbleibt es bei der Anwendung der DSGVO bzw. dem BDSG.[5] 195

Das KDG gilt darüber hinaus nicht im Bereich der **Ordensgemeinschaften** päpstlichen Rechts und im Bereich der von diesen ganz oder mehrheitlich getragenen Werke und Einrichtungen ohne Rücksicht auf deren zivile Rechtsformen.[6] 200

Das KDG findet aber dann Anwendung, wenn Unternehmen durch **Outsourcing** entstanden sind und sich weiterhin im Eigentum kirchlicher Rechtsträger befinden. 205

**BEISPIEL**

Ein Krankenhaus gliedert den Reinigungsdienst auf eine separate Gesellschaft aus. Alleiniger (oder mehrheitlicher) Eigentümer bleibt aber der kirchliche Rechtsträger. Wenn diese Reinigungsgesellschaft nicht werbend am Markt tätig wird, sondern ausschließlich für kirchliche Einrichtungen tätig ist, unterfällt sie der Zuständigkeit des KDG. 210

1 Ehmann/Selmayr, DSGVO 2. Auflage 2018 Rn. 12
2 BVerfG, Urteil vom 11.10.1977, 2 BvR 209/76 (43, 76)
3 Seifert in Simitis, Art. 91 Rn. 2; 2. Tätigkeitsbericht Diözesandatenschutzbeauftragter der ostdeutschen Bistümer S. 11, abzurufen unter www.datenschutzbeauftragter-ost.de
4 BeckOK Datenschutzrecht, Wolff/Brink 28. Edition (Stand 1.2.2017), Rn. 11
5 Gola, DSGVO 2. Auflage 2018, Rn.1
6 § 3 Kirchliche KDR-OG

215 Anders wäre der Fall zu beurteilen, wenn die Reinigungsgesellschaft zwar im Eigentum kirchlicher Träger verbleibt, aber als werbendes Unternehmen mit Gewinnerzielungsabsicht am Markt tätig wird. Dann gelten die staatlichen Datenschutzvorschriften, weil die wirtschaftliche Betätigung im Vordergrund steht. Staatliches Datenschutzrecht gilt auch dann, wenn der Reinigungsdienst an private Eigentümer ausgegliedert wird, selbst dann, wenn diese ausschließlich das Krankenhaus reinigen.

### 1.7 Datenschutzaufsicht

220 Art. 91 Abs. 2 DSGVO legt fest, dass Religionsgemeinschaften, die umfassende Datenschutzregeln anwenden, einer unabhängigen Aufsichtsbehörde unterliegen. Das gilt unabhängig davon, ob die Religionsgemeinschaft eigenes Datenschutzrecht anwendet oder die DSGVO.[1] Auch ist damit zunächst noch nicht zwingend festgelegt, dass diese in der Verordnung erlaubte spezifische Aufsicht eine solche der Kirche selber sein muss. Denkbar wäre es auch, spezielle staatliche Stellen mit der Aufsicht über die Religionsgemeinschaften zu betrauen.[2] Art. 91 DSGVO gewährt den Religionsgemeinschaften eine Souveränität, die durch eine staatliche Aufsicht aber wieder aberkannt würde. Insbesondere durch die der Aufsicht eingeräumten Rechte - freier Zugang zu den Einrichtungen, Einsicht in Unterlagen u.a. - würde den Religionsgemeinschaften mit der einen Hand wieder weggenommen werden, was mit der anderen gegeben wurde. So liegt es näher Abs. 2 so zu verstehen, dass durch diese Vorschrift die Errichtung kircheneigener Aufsichtsbehörden ermöglicht wird.[3]

225 Dies wird auch durch die Bundesbeauftragte für Datenschutz und Informationsfreiheit so konstatiert, wenn sie feststellt: *„Diese Vorschrift erlaubt es den Kirchen, eine spezifische Art der Datenschutzaufsicht vorzusehen. Damit können die Kirchen in Deutschland mit ihren eigenen kirchlichen Datenschutzbeauftragten insoweit ihre verfassungsrechtlich und europarechtlich geschützte Autonomie weiterhin ausüben. Die kirchlichen Datenschutzbeauftragten müssen allerdings die Bedingungen des Kapitel VI der Datenschutz-Grundverordnung erfüllen. Auch sie müssen daher unabhängig sein, ihnen müssen eine angemessene Ausstattung zur Verfügung gestellt sowie bestimmte Aufgaben und Befugnisse eingeräumt werden“.*[4]

230 Die kircheneigene Aufsichtsorganisation ist nicht per se minderer Qualität.[5] Dies gilt jedenfalls dann, wenn sie den Anforderungen des VI. Kapitels der DSGVO entspricht. Diese Entsprechung ist durch die Vorschriften im 6. Kapitel des KDG gewährleistet.

1 Paal/Pauly, Art. 91 Rn. 30
2 BeckOK Datenschutzrecht, Wolff/Brink, 28. Edition Stand 1.2.2017, Art. 91 Rn. 22; Paal/Pauly, Art. 91 Rn. 30
3 Seifert in Simitis, Art. 91 Rn. 24.
4 Info 6, S. 31
5 Hense in Sydow, Art. 91 Rn. 27

Zunächst ist die dort geregelte Datenschutzaufsicht von dem **betrieblichen** Datenschutzbeauftragten zu unterscheiden. Letzterer untersteht dem Leiter der Stelle, die ihn bestellt hat. Der Diözesandatenschutzbeauftragte als Leiter der kirchlichen Datenschutzaufsicht ist unabhängig. Es ist zu gewährleisten, dass er seine Tätigkeit frei von Weisungen ausüben kann, § 43 Abs. 1 KDG. Eine Abberufung des Diözesandatenschutzbeauftragten vor Ablauf seiner Amtszeit ist nur möglich, wenn Gründe nach § 24 Deutsches Richtergesetz[1] vorliegen, die auch bei einem auf Lebenszeit eingestellten Richter eine Entlassung rechtfertigen würden. Er ist hauptamtlich tätig, § 43 Abs. 2 KDG. Ihm wird für die Erfüllung seiner Aufgaben die notwendige Personal- und Sachausstattung zur Verfügung gestellt, § 43 Abs. 4 KDG. Unabhängig davon, ob das Personal von der Datenschutzaufsicht selber oder von einer anderen kirchlichen Stelle angestellt wird, wählt der Diözesandatenschutzbeauftragte das notwendige Personal selber aus. Das Personal untersteht ausschließlich der Dienst- und Fachaufsicht des Diözesandatenschutzbeauftragten, § 43 Abs. 5 KDG. 235

Die dem KDG gem. § 3 Abs. 1 unterworfenen Einrichtungen sind verpflichtet, den Anweisungen der Datenschutzaufsicht Folge zu leisten und diese bei Erfüllung ihrer Aufgaben zu unterstützen. Dabei ist der Datenschutzaufsicht insbesondere Einsicht in alle Unterlagen und Akten zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Der Datenschutzaufsicht ist Zutritt zu allen Diensträumen zu gewähren, die der Verarbeitung und der Aufbewahrung automatisierter Dateien dienen (§ 44 Abs. 2 KDG). 240

Anders als nach der bisherigen Rechtslage ist die Datenschutzaufsicht nicht mehr darauf beschränkt, Beanstandungen gegenüber dem Verantwortlichen auszusprechen, sondern „kann“ gem. § 51 KDG auch **Geldstrafen** verhängen. 245

Während der Wortlaut des Art. 83 Abs. 2 Satz 1 DSGVO für eine Pflicht zur Verhängung einer Geldstrafe spricht und Erwägungsgrund 148 von einer solchen nur in dort genannten Ausnahmefällen abzusehen empfiehlt,[2] spricht das KDG mit der „Kann“-Vorschrift in § 51 eine deutlich weichere

1 *„Wird gegen einen Richter durch Urteil eines deutschen Gerichts im Geltungsbereich dieses Gesetzes erkannt auf*
*1. Freiheitsstrafe von mindestens einem Jahr wegen einer vorsätzlichen Tat,*
*2. Freiheitsstrafe wegen einer vorsätzlichen Tat, die nach den Vorschriften über Friedensverrat, Hochverrat, Gefährdung des demokratischen Rechtsstaates oder Landesverrat und Gefährdung der äußeren Sicherheit strafbar ist,*
*3. Aberkennung der Fähigkeit zur Bekleidung öffentlicher Ämter oder*
*4. Verwirkung eines Grundrechts gemäß Artikel 18 des Grundgesetzes,*
*so endet das Richterverhältnis mit der Rechtskraft dieses Urteils, ohne dass es einer weiteren gerichtlichen Entscheidung bedarf.“*

2 Ehmann/Selmayr, DSGVO, 2. Auflage 2018, Rn. 14; Boehm in Simitis, Art. 83 Rn. 15; a. A. Paal/Pauly, Art 83 Rn. 10

Sprache. Interessant in diesem Zusammenhang ist, dass sich der europäische Normgeber in den Trilogverhandlungen genau von einer solchen „Kann-Formulierung" verabschiedet hat.[1] Im Sinne eines „In-Einklang-Bringens" der kirchlichen Regelung mit denen der DSGVO wird man davon ausgehen müssen, dass die Verhängung einer Geldstrafe nach § 51 KDG trotz des dort enthaltenen Begriffs „kann" die Regel ist. Ein Absehen von einer Geldbuße kommt nur dann in Betracht, wenn diese gegen eine natürliche Person verhängt werden müsste und für die Person eine unverhältnismäßige Belastung darstellen würde. Ebenso dann, wenn der Verstoß nur geringfügig ist, was letztlich dem Verhältnismäßigkeitsgrundsatz entspricht.[2]

250 Jede betroffene Person kann sich an die kirchliche Datenschutzaufsicht wenden. Die Tätigkeit der Datenschutzaufsicht ist zunächst für Betroffene kostenlos. Im Falle offensichtlich unbegründeter oder exzessiver Anfragen kann die Datenschutzaufsicht eine weitere Tätigkeit von der Zahlung einer Verwaltungsgebühr abhängig machen.

255 Jede kirchliche Datenschutzaufsicht ist verpflichtet, einen jährlichen Tätigkeitsbericht zu erstellen, der dem Bischof vorzulegen ist, und darüber hinaus diesen Bericht zu veröffentlichen.[3] Inhalt dieser Tätigkeitsberichte ist neben der Darstellung der Entwicklung des Datenschutzes im staatlichen und kirchlichen Bereich auch eine zumindest beispielhafte Darstellung der im Berichtsjahr behandelten Datenschutzverstöße.

## 2. Grundlagen des Datenschutzes

### 2.1 Grundsätze der Datenverarbeitung

260 Der zentrale Grundsatz des Datenschutzes ist die **Verpflichtung zur Zweckbindung.** Dadurch soll gewährleistet werden, dass der betroffenen Person bekannt ist, wer, was, wann, bei welcher Gelegenheit und in welchem Umfang über sie weiß.[4] Dadurch soll auch die Transparenz der Datenverarbeitung sichergestellt werden. Der Zweck muss „festgelegt" sein. Das bedeutet, der Zweck muss bereits bei Erhebung der Daten bestehen.

1 Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Rn. 32
2 So auch für die staatliche Regelung Schreibauer/Spittka in Wybitul, Art. 83 Rn. 13
3 Tätigkeitsberichte sind auf den Homepages der Diözesandatenschutzbeauftragten eingestellt: www.katholisches-datenschutzzentrum.de; www.datenschutz-kirche.de; datenschutzbeauftragter-ost.de; www.kath-datenschutzzentrum-ffm.de
4 BVerfGE 65, 1 ff (43, 45)

**BEISPIEL**

Auf Personalbogen werden neue Mitarbeitende gelegentlich gefragt, ob sie verheiratet sind und seit wann. Darüber hinaus wird nach der kirchlichen Eheschließung und dem Datum gefragt. Während die Frage nach der Eheschließung aus steuerlichen Gründen erforderlich ist, besteht für die Frage „seit wann" zunächst kein Zweck im Zeitpunkt der Erhebung. Gerechtfertigt wird dies mit einer Regelung in den kirchlichen Tarifbestimmungen. Danach gibt es einen Tag Arbeitsfreistellung bei Feier der Silberhochzeit. 265

Die Erhebung dieses Datums ist nicht durch einen Zweck gedeckt, da der Zweck in der Zukunft liegt und nicht sicher ist, ob der Mitarbeiter dann noch in der Einrichtung tätig ist. Auch sind Mitarbeitende nicht verpflichtet, diese Arbeitsbefreiung in Anspruch zu nehmen. Diese Angabe ist bestenfalls unter Freiwilligkeitsvorbehalt zu erheben. 270

Ausreichend ist es ferner, dass Mitarbeitende ihren Anspruch geltend machen, wenn das Ehejubiläum unmittelbar ansteht. Die Frage auf dem Personalbogen ist nicht durch einen konkreten Zweck gedeckt und damit unzulässig. Für die Frage nach einer kirchlichen Eheschließung gilt das gleiche wie für die Frage nach der Religionszugehörigkeit.

Häufig wird im Zusammenhang mit Bewerbungen noch nach der Religionszugehörigkeit gefragt. In Folge der Rechtsprechung des Europäischen Gerichtshofs darf die Religionszugehörigkeit aber als **Voraussetzung für eine Einstellung** nicht mehr für jede Stelle pauschal verlangt werden. Der EuGH verlangt dagegen einen objektiv überprüfbaren direkten Zusammenhang zwischen der Religionszugehörigkeit und der fraglichen Tätigkeit. Dieser kann sich aus der Art der Tätigkeit (z. B. Aufgaben der Verkündigung) oder aus den Umständen ihrer Ausübung ergeben. Dies wird insbesondere bei Leitungspositionen der Fall sein, in denen der Amtsinhaber die Position der Kirche glaubwürdig vertreten muss (etwa Leitung einer katholischen Kindertagestätte oder anderer kirchlicher Einrichtungen).[1] Aufgrund dieser Rechtsprechung fehlt für die pauschale Frage nach der Religionszugehörigkeit der Zweck. Demgegenüber ist die Frage auf einem Personalbogen aber von einem Zweck getragen, wenn der Arbeitgeber verpflichtet ist, im Falle der Religionszugehörigkeit Kirchensteuern abzuführen. 275

Grundsätzlich verfolgt jede Datenverarbeitung einen Zweck. Dieser muss aber nach den Vorgaben des Gesetzes legitim sein, also bestimmten Rechtsregeln folgen. Dementsprechend muss die Datenverarbeitung zur Erreichung des Zwecks erforderlich sein. Das bedeutet, der Zweck der Verarbeitung kann nicht auf zumutbare Weise durch andere Mittel erreicht 280

1 Amtsblatt Bistum Magdeburg vom 1.7.2019, Nr. 78

werden.[1] Der Zweck muss eindeutig bestimmt sein, was die Verwendung von **Blankettformeln** ausschließt.

### 2.2 Datenminimierung

285 Der Grundsatz der Datenminimierung ergibt sich aus § 7 Abs. 1 lit. c KDG (Art. 5 Abs. 1 lit c DSGVO). Danach ist die Verarbeitung solcher Daten verboten, die dem Zweck nicht angemessen und erheblich sowie auf das notwendige Maß beschränkt sind.

290 Angemessen sind solche Daten, die dem Zweck adäquat sind, ihm also entsprechen.[2] Erheblichkeit ist gegeben, wenn die Daten für irgendeinen Aspekt des Zwecks entscheidend sind.[3] Die Beschreibung „auf das erforderliche Maß beschränkt" ist gleichzusetzen mit dem Begriff erforderlich. Das heißt, ohne diese Daten kann der Verantwortliche den Zweck nicht, nicht vollständig oder nur mit unverhältnismäßigem Aufwand erfüllen[4].

295 Im Ergebnis fordert § 7 Abs. 1 lit c, personenbezogene Daten nur dann zu verarbeiten, wenn keine Alternative zur Verwendung dieser Daten besteht.[5] Eine Alternative besteht nach dem Gesetz vor allem dann, wenn die verwendeten Daten auch anonymisiert oder pseudonymisiert verwendet werden könnten. Danach besteht ein Personenbezug dann nicht mehr.

### 2.3 Datengeheimnis

300 In § 5 KDG wird das Datengeheimnis legal definiert: *„Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten."* Weiterhin ist in dieser Vorschrift ausdrücklich die Pflicht geregelt, Personen, die mit Datenverarbeitung beschäftigt sind, bei der Aufnahme ihrer Tätigkeit schriftlich auf das Datengeheimnis zu verpflichten. Diese Vorschrift entspricht inhaltlich weitgehend § 4 KDO sowie § 5 BDSG a. F.

305 Adressat dieser Verpflichtung sind gem. § 2 KDG-DVO alle Beschäftigten gem. § 4 Nr. 24 KDG der in § 3 Abs. 1 KDG genannten Einrichtungen. Wegen des Schutzzwecks der Norm ist der Anwendungsbereich weit auszulegen.[6] Erfasst werden deshalb alle Mitarbeitende, denen die ihnen zugewiesene Tätigkeit eine Möglichkeit verschafft, Zugang zu personenbezogenen Daten zu erlangen. Ob ein tatsächlicher Umgang erfolgt, ist primär nicht entscheidend.[7]

1 Erwägungsgrund 35
2 Reimer in Sydow, Art. 5 Rn. 30
3 Roßnagel in Simitis, Art. 5 Rn. 120
4 Kühling/Buchner, Art. 6 Rn. 45; Gola/Schomerus, § 28 Rn. 15
5 Heidelberger Kommentar, Art. 5 Rn. 48
6 Däubler/Klebe/Wedde/Weichert (DKWW), Kommentar zum BDSG a. F, 5. Auflage 2016, § 5 Rn. 4
7 Bergmann/Möhrle/Herb, Datenschutzrecht (Stand Februar 2015) zu BDSG a. F.

Unbefugt handeln Mitarbeitende bereits dann, wenn zwar die Verarbeitung aus Sicht des Verantwortlichen zulässig ist, sie aber die ihnen intern zugewiesenen Zugriffsberechtigungen überschreiten.[1] Ein Verstoß stellt z. B. die Verarbeitung von Daten zu persönlichen Zwecken dar, wie das Sammeln von Eingruppierungsdaten von anderen Mitarbeitenden, um damit ggf. einen eigenen Höhergruppierungsantrag begründen[2] zu können, oder die Verwendung von Kontaktdaten aus der Personalakte zur persönlichen Kontaktaufnahme sowie wiederholter Abruf von Meldedaten ohne dienstliche Veranlassung. 310

Derartige Verstöße können darüber hinaus dazu führen, dass der handelnde Mitarbeiter selber Verantwortlicher i. S. d. § 4 Nr. 9 KDG wird, weil er entgegen der Weisung der Einrichtungsleitung personenbezogene Daten verarbeitet und damit die vorgegebene Zweckbindung übertritt und selber über Zweck und Mittel bestimmt. Gegen einen Mitarbeitenden, der sich selber zum Verantwortlichen macht, können Sanktionen gem. § 51 KDG direkt verhängt werden.[3] 315

Die Verpflichtung auf das Datengeheimnis ist erforderlich, damit Mitarbeitende ihre Pflichten kennen und sich nicht auf einen Verbotsirrtum berufen können.[4] Die Mitteilung des Gesetzeswortlautes reicht dafür ebenso wenig aus wie ein entsprechender Aushang am „Schwarzen Brett". Erforderlich ist also eine arbeitsplatzbezogene, individuelle Belehrung (§ 3 Abs. 1 lit. b KDG-DVO). 320

Die Verpflichtung der Beschäftigten hat zu erfolgen, bevor die Verarbeitung personenbezogener Daten aufgenommen wird. Soweit Mitarbeitende nach den Vorschriften § 4 KDO belehrt worden sind und diese Belehrung inhaltlich den Anforderungen des § 5 KDG entspricht, ist eine erneute Verpflichtung nicht erforderlich. 325

Die nach § 5 KDG schriftlich abzugebende Verpflichtungserklärung geht also über die in den **§§ 5 und 5a AVR AT geregelte Verschwiegenheitsverpflichtung** hinaus, weil sie einen eigenen Erklärungsinhalt aufweist, und ist deshalb neben den AVR-Regelungen gesondert abzugeben. 330

Zu den möglichen rechtlichen Folgen, auf die Mitarbeitende in der Verpflichtungserklärung hinzuweisen sind, gehören neben einer Sanktionierung durch die Datenschutzaufsicht auch die Möglichkeit der Sanktionierung durch den Dienstgeber in Form von Abmahnung oder Kündigung.[5] 335

1 Franzen in Erfurter Kommentar, 18. Auflage zu § 5 BDSG a.F. Rn. 1
2 DKWW, § 5 Rn. 9
3 Caumanns, RdV 2018, 55
4 Gola/Schomerus, § 5 Rn. 4
5 LAG Berlin-Brandenburg, Urteil vom 1.9.2016, 10 Sa 192/16

340 **Muster: Verpflichtungserklärung zum Datengeheimnis gemäß § 5 KDG**

*Ich, *Name* bin bei/ in *Dienststelle* als *Tätigkeit* hauptamtlich/ehrenamtlich tätig.*

*Ich verpflichte mich,*

*1. zur Einhaltung des Datengeheimnisses (§ 5 KDG) und zur Einhaltung des kirchlichen Datenschutzgesetzes und der dazu erlassenen Verordnungen in der jeweils geltenden Fassung;*

*2. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten.*

*Darüber hinaus bestätige ich, dass ich auf die folgenden, für die Ausübung meiner Tätigkeit spezifischen, geltenden Bestimmungen, *Aufzählung der spezifischen Gesetze* hingewiesen wurde, und versichere deren Einhaltung. Die Möglichkeit der Einsichtnahme und Ausleihe dieser Texte wurden mir mitgeteilt.*

*Ich bin darüber belehrt worden, dass ein Verstoß gegen das KDG und die anderen für meine Tätigkeit geltenden Datenschutzvorschriften rechtliche Folgen haben kann.*

*Ort, Datum, Unterschrift*

345 Eine solche Regelung findet man in der DSGVO und dem BDSG[1] nicht direkt. Dennoch ist sie auch nach der neuen Gesetzeslage im staatlichen Bereich nicht obsolet.

350 Art. 5 DSGVO bestimmt die Grundsätze der Datenverarbeitung, nach denen u. a. Daten auf rechtmäßige Weise nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Die in Abs. 2 normierte Rechenschaftspflicht legt dem Verantwortlichen die Pflicht auf, die Einhaltung der Grundsätze nachweisen zu können.

355 Art. 29 DSGVO legt fest, dass dem Verantwortlichen und dem Auftraggeber unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese ausschließlich nur auf Weisung verarbeiten dürfen. Damit die Umsetzung dieser Verpflichtung gewährleistet wird, fordert Art. 32 DSGVO den Verantwortlichen und den Auftragsverarbeiter dazu auf, entsprechende Schritte zu unternehmen, die die Umsetzung der Verpflichtung sicherstellen. Schließlich verlangt Art. 24 Abs. 1 DSGVO vom Verantwortlichen den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

1 § 53 BDSG enthält zwar in der Überschrift die Bezeichnung „Datengeheimnis“, ist jedoch für Unternehmen und sonstige private Stellen nicht anwendbar. Dies wird deutlich aus der Überschrift des Teils 3 BDSG, der darauf hinweist, dass mit den folgenden Regeln nicht die DSGVO, sondern die Richtlinie (EU) 2016/680 umgesetzt werden soll.

Daraus folgt, dass es zwar in der DSGVO keine ausdrückliche Regelung für eine förmliche Verpflichtung auf das Datengeheimnis gibt, es aber aufgrund der zitierten Vorschriften angeraten ist, an einer dokumentierten Verpflichtung festzuhalten, um der Rechenschaftspflicht genügen zu können. Eine Verschärfung im kirchlichen Datenschutzrecht gegenüber den staatlichen Regelungen liegt insoweit also nicht vor. 360

## 2.4 Einwilligung

Definiert wird die Einwilligung in § 4 Nr. 13 KDG. In § 6 Abs. 1 wird die Einwilligung als eine neben anderen Möglichkeiten bestehender Rechtmäßigkeitsvoraussetzungen benannt. Häufig wird die Einwilligung vom Verantwortlichen als die sicherste Rechtmäßigkeitsvoraussetzung betrachtet, da sich ihm die anderen Voraussetzungen inhaltlich nur schwer erschließen und der Verantwortliche sich deshalb mit der Subsumtion unter die jeweiligen Tatbestände schwertut. Vor diesem Hintergrund erscheint die Abforderung einer Einwilligung zwar verlockend, zu beachten ist aber, dass dieser vermeintliche Vorteil mit einer nicht unerheblichen Rechtsunsicherheit erkauft wird, da die Einwilligung immer unter dem Vorbehalt der jederzeitigen Widerruflichkeit steht. 365

Die Einwilligung muss zunächst von der betroffenen Person selbst abgegeben werden. Sie ist also eine **höchstpersönliche Erklärung.**[1] Dabei ist es ausreichend, dass diese über die entsprechende Einsichtsfähigkeit verfügt, dementsprechend kommt es nicht auf die Geschäftsfähigkeit an.[2] Erklärungen, die durch Ehegatten für den anderen Teil abgegeben werden, scheiden deshalb ebenso aus wie eine Einwilligung von Freunden oder Kollegen. 370

### 2.4.1 Freiwilligkeit

Die Einwilligung muss freiwillig, also unter Abwesenheit von Zwang, Druck oder Abhängigkeitslagen erfolgen. Insbesondere im Beschäftigungszusammenhang ist deshalb an die Freiwilligkeit der Einwilligung ein besonderer Maßstab anzulegen. Im staatlichen Bereich ist dies in § 26 BDSG ausdrücklich dargestellt. § 26 Abs. 2 BDSG fordert für die Beurteilung der Freiwilligkeit einer Einwilligungserklärung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Eine dementsprechende Formulierung ist im KDG nicht aufgenommen, gleichwohl ist diese Abhängigkeitslage auch im kirchlichen Dienstverhältnis zu beachten. Dem steht die Tatsache, dass es sich in diesem Verhältnis um eine Dienstgemeinschaft handelt, nicht entgegen. 375

1 Ernst in Paal/Pauly, Art. 4 Rn. 65
2 Däubler, Gläserne Belegschaften, 8. Auflage 2019, Rn. 138

380 Die Einwilligung ist für den bestimmten Fall abzugeben. Damit ist festgestellt, dass es keine **Generaleinwilligungen** geben kann. Jede Einwilligung muss erkennen lassen, welche personenbezogenen Daten zu welchem Zweck von wem verarbeitet werden.[1]

### 2.4.2 Form

385 Eine Einwilligung nach § 8 KDG bedarf zu ihrer Wirksamkeit der Schriftform. Dies entspricht der alten Rechtslage in § 3 Abs. 2 KDO sowie dem BDSG (§ 4a Abs. 1 S. 3). Während die DSGVO auf jedes Formerfordernis für die Einwilligung verzichtet, erhält das KDG diese Anforderung aufrecht. Gem. § 126 BGB ist für die Schriftform die **eigenhändige Unterschrift** erforderlich. Nicht ausreichend ist die in § 126 b BGB definierte Textform, also eine lesbare Erklärung, in der die Person des Erklärenden genannt und auf einem dauerhaften Datenträger abgegeben ist. Die Textform ist der Schriftform jedoch nicht gleichgestellt und in § 8 Abs. 2 KDG nicht erwähnt.

390 Für eine wirksame Einwilligungserklärung per E-Mail müsste diese mit einer qualifizierten elektronischen Signatur versehen sein. Eine solche Signatur, die den Anforderungen des § 2 Signaturgesetz entsprechen müsste, ist im privaten Rechtsverkehr unüblich, weshalb an dieser Stelle auf die Einzelheiten nicht einzugehen ist.

395 Eine Ausnahme besteht in den Fällen, in denen wegen besonderer Umstände eine andere Form angemessen ist. Im Rahmen von Arbeitsverhältnissen dürften solche besonderen Umstände kaum vorkommen. Auf jeden Fall ist aber auch in diesen Fällen ein aktives Tätigwerden der betroffenen Person erforderlich. In keinem Fall kann eine Einwilligung aus der Untätigkeit einer betroffenen Person hergeleitet werden.

**BEISPIEL**

400 *„Wir gehen davon aus, dass Sie mit der Bekanntgabe Ihrer Mobilfunknummer an unsere Klienten einverstanden sind, sofern Sie diesem Vorgehen nicht widersprechen. “*

Hier gilt der Rechtsgrundsatz „Wer schweigt, erklärt nichts.“ Aus einer Untätigkeit auf diese Aufforderung auf eine Zustimmung zu schließen, würde ein unzulässiges „opt-out-Verfahren“ darstellen.

1 Ernst in Paal/Pauly, Art. 4 Rn. 78

### 2.4.3 Widerruf

§ 8 Abs. 6 Satz 1 KDG gewährt der betroffenen Person ein jederzeitiges Widerrufsrecht der Einwilligung. Diese Regelung war im alten Recht der KDO nicht ausdrücklich festgeschrieben, wurde aber seinerzeit als selbstverständlich betrachtet. Gleichzeitig wird dem Verantwortlichen die Pflicht auferlegt, die betroffene Person vor Abgabe der Einwilligung auf den Umstand der Widerruflichkeit in Kenntnis zu setzen (Satz 3). Dieser Hinweis ist damit Wirksamkeitsvoraussetzung für die Einwilligungserklärung.[1]

Der Widerruf ist gegenüber dem Verantwortlichen gem. § 4 Nr. 9 abzugeben. Der Verantwortliche selbst hat dafür zu sorgen, dass der Widerruf an die ggf. zuständige Stelle in der Einrichtung weitergeleitet wird. Der Widerruf der Einwilligung bedarf weder einer besonderen Form noch einer Begründung. Allein der Wille der betroffenen Person, die ursprünglich erteilte Einwilligung nicht mehr gegen sich gelten lassen zu wollen, ist ausreichend. Das gilt auch dann, wenn die Einwilligung nicht ausdrücklich erklärt wurde, aber aus dem schlüssigen Verhalten der betroffenen Person ein solcher Wille zu schließen ist (konkludente Erklärung). Dabei kommt es auf eine Freiwilligkeit nicht an (z.B. Mutter widerruft eine Fotoerlaubnis unter Hinweis darauf, dass ihr der Vater des Kindes andernfalls mit einem Sorgerechtsstreit droht.)

Durch den Widerruf wird die Verarbeitung der personenbezogenen Daten ab dem Eingang des Widerrufs **für die Zukunft** unrechtmäßig. Das Gesetz formuliert an dieser Stelle ausdrücklich, dass der Widerruf keine Auswirkung auf die bis zu seinem Eingang durchgeführte Verarbeitung hat.

**BEISPIEL**

Eine Einrichtung gibt eine Festschrift zum 50-jährigen Bestehen heraus, in der auch Fotos von Mitarbeitern abgebildet sind. Dabei handelt es sich um die Verarbeitung personenbezogener Daten, für die eine Einwilligung mangels anderer Rechtsgrundlage erforderlich ist. Haben diese Einwilligungen bei Drucklegung vorgelegen, dürfen die gedruckten Exemplare weitergegeben werden, auch wenn eine abgebildete Person ihre Einwilligung nach dem Druck widerrufen hat. Die gedruckten Exemplare müssen nicht vernichtet werden und schon gar nicht sind verteilte Exemplare zurückzurufen.

Anders verhält es sich, wenn Fotos auf einer Homepage eingestellt sind und die abgebildete Person ihre ursprünglich erteilte Einwilligung widerruft. In diesem Fall hat eine Löschung oder Unkenntlichmachung auf der Homepage unverzüglich zu erfolgen.

1 Klement in Simitis, Art. 7 Rn. 95

### 2.4.4 Kopplungsverbot

430 Das Kopplungsverbot nach Abs. 7 stellt einen speziellen Fall der nicht freiwilligen Einwilligung dar. Freiwillig ist eine Einwilligung, wenn die betroffene Person eine echte, freie Wahl hat darüber zu entscheiden, die Einwilligung abzugeben oder zu verweigern, ohne dadurch Nachteile zu erleiden.[1] Deshalb darf der Abschluss eines Vertrages nicht davon abhängig gemacht werden, in die Verarbeitung personenbezogener Daten einzuwilligen, die für die Erfüllung des Vertrages nicht erforderlich ist.

**BEISPIEL**

435 Der Dienstgeber lässt sich bei der Einstellung im Arbeitsvertrag die Einwilligung dafür unterschreiben, dass Fotos Mitarbeitender auf der Homepage und in Werbebroschüren der Einrichtung veröffentlicht werden dürfen.

Bei der Veröffentlichung von Fotos handelt es sich um personenbezogene Daten. Für die Erfüllung der Verpflichtungen aus einem Arbeitsvertrag ist eine solche Erlaubnis regelmäßig nicht erforderlich. Die Kopplung der Einwilligung an den Abschluss des Arbeitsvertrages ist unzulässig, eine entsprechend erteilte Einwilligung also unwirksam.

440 Im vorliegenden Fall gilt dies bereits deshalb, weil im Verhältnis Dienstgeber./.Dienstnehmer ein besonderes Ungleichgewicht besteht.[2] Gerade für Einwilligungen im Zusammenhang mit einem Arbeitsverhältnis ist bei der Prüfung der Freiwilligkeit darauf abzustellen, ob der Dienstnehmer einen rechtlichen oder wirtschaftlichen Vorteil durch die Einwilligung erlangt oder Dienstgeber und Dienstnehmer gleichgerichtete Interessen verfolgen.[3] Eine derartige Interessenlage wird ausschließlich auf solche Daten beschränkt sein, an deren Kenntnis der Dienstgeber ein berechtigtes Interesse hat.[4] Insbesondere fallen Daten zum Privatleben einschließlich politischer oder gewerkschaftlicher Betätigungen ebenso wenig darunter, wie die familiären oder finanziellen Verhältnisse des Mitarbeitenden.

### 2.4.5 Alteinwilligungen

445 Wenn der Verantwortliche personenbezogene Daten aufgrund einer Einwilligung verarbeitet, die auf der Grundlage der KDO (§ 3 Abs. 2) erfolgt ist, kann diese Einwilligung der aktuellen Verarbeitung personenbezo-

1 Erwägungsgrund 42
2 Erwägungsgrund 43
3 Diese Regelung ist in § 26 BDSG ausdrücklich festgeschrieben. Im KDG fehlt ein solcher Hinweis, dennoch kann die staatliche Regelung bei der Auslegung der Frage nach der Freiwilligkeit herangezogen werden.
4 Däubler, Rn. 166

gener Daten zugrunde gelegt werden, wenn sie den Regelungen des § 8 KDG entspricht. Das wird dann nicht der Fall sein, wenn der Einwilligung der Hinweis auf die jederzeitige Widerrufbarkeit fehlt. Ebenso dann, wenn die Einwilligung besondere Kategorien personenbezogener Daten umfasst und die Einwilligung sich nicht ausdrücklich auf diese bezieht.

### 2.4.6 Einwilligung neben gesetzlicher Rechtsnorm

Nach § 6 Abs. 1 Satz 1 KDG ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn mindestens eine der dort aufgeführten Bedingungen erfüllt ist. Unter lit. b ist an dieser Stelle die Einwilligung genannt. Diese steht neben den anderen Bedingungen.[1] Dem Verantwortlichen steht es also zunächst frei, die Verarbeitung auf eine Einwilligung zu stützen, obwohl er sich auf einen anderen Zulässigkeitstatbestand hätte berufen können. Insoweit kann die vorsorglich eingeholte Einwilligung gerade vor dem Hintergrund der Unbestimmtheit der gesetzlich formulierten Erlaubnistatbestände zu mehr Rechtssicherheit führen. 450

Fraglich ist, ob die Verarbeitung auch dann noch auf einen gesetzlichen Erlaubnistatbestand gestützt werden kann, wenn eine Einwilligung eingeholt worden ist. Dies könnte im Falle des Widerrufs der Einwilligung dazu führen, dass der Verantwortliche die Verarbeitung fortsetzt und sich dabei auf einen gesetzlichen Zulässigkeitstatbestand stützt. Der betroffenen Person müsste dieses Verhalten als widersprüchlich erscheinen, wurde ihm doch durch die Einholung der Einwilligung suggeriert, dass die Verarbeitung seiner personenbezogenen Daten von seiner Zustimmung abhängt.[2] § 19 Abs. 1 lit. b legt nahe, dass der gesetzliche Erlaubnistatbestand nicht entfällt, wenn die Einwilligung widerrufen wird oder sich als unzulässig erweist.[3] Zu berücksichtigen ist aber, dass der kirchliche Normgeber sich anders als der europäische entschieden hat, die Einwilligung erst an zweite Stelle (lit. b) zu stellen, hinter dem Erlaubnistatbestand der kirchlichen oder staatlichen Rechtsvorschrift (lit. a). 455

Da ein gleichlautender Erlaubnistatbestand in der europäischen Norm fehlt, dürfte davon auszugehen sein, dass das KDG hier eine Rangfolge festschreibt. Davon unabhängig ist aber in § 8 Abs. 1 KDG gefordert, dass die betroffene Person, soweit nach den Umständen erforderlich, auf die Folgen einer Verweigerung der Einwilligung hinzuweisen ist. An dieser Stelle ist klar, dass die betroffene Person auf den parallel bestehenden gesetzlichen Erlaubnistatbestand hinzuweisen ist und ihre Einwilligung in diesem Fall nur einen deklaratorischen Hinweischarakter besitzt.[4] Fehlt 460

1 Klement in Simitis, DSGVO, Art. 7 Rn. 34
2 Buchner/Kühling, Rn. 18
3 Klement in Simitis, Art. 7 Rn. 34
4 Im Ergebnis für das europäische Recht: Buchner/Kühling, Rn. 18

der Verweis auf die Folgen der Verweigerung der Einwilligung oder wird nicht hinreichend dargestellt, dass neben der Einwilligung ein gesetzlicher Rechtmäßigkeitsgrund für die Verarbeitung besteht, wird bei der betroffenen Person eine falsche Vorstellung über die Tragweite ihrer Einwilligung entstehen. Die Einwilligung wäre in diesem Fall ohnehin unwirksam.[1]

## 3. Betrieblicher Datenschutzbeauftragter

465 Gem. § 36 Abs. 1 KDG sind alle Einrichtungen des verfasst kirchlichen Bereichs, also Ordinariate, Pfarreien, Kirchengemeinden, Kirchenstiftungen, unabhängig vom Vorliegen weiterer Bedingungen verpflichtet, einen betrieblichen Datenschutzbeauftragten zu benennen. Im staatlichen Bereich gilt Gleiches gem. § 37 Abs. 1 lit. a für Behörden.

470 Die anderen in § 3 Abs. 1 KDG genannten Einrichtungen, also auch die Caritaseinrichtungen, benennen einen betrieblichen Datenschutzbeauftragten unter den Voraussetzungen des § 36 Abs. 2 KDG, die Art. 37 Abs. 1 lit. b und c DSGVO und § 38 BDSG entsprechen. Danach legt § 36 Abs. 2 lit a KDG eine Ausnahme von der Benennungspflicht fest, die durch die folgenden lit. b und c wieder relativiert wird.

475 Einrichtungen, die **weniger als zehn Personen** mit der Verarbeitung personenbezogener Daten beschäftigen, müssen keinen betrieblichen Datenschutzbeauftragten bestellen. Im Unterschied zu der alten Regelung der KDO ist der Grenzwert um eine Person reduziert worden.[2] Weiterhin ist nach der jetzt geltenden Fassung keine automatisierte Verarbeitung erforderlich, sondern jede Verarbeitung personenbezogener Daten i. S. v. § 2 Abs. 1 ist ausreichend.[3] Die Zahl von mindestens zehn Personen ist „in der Regel" zu erreichen. Das bedeutet, eine vorübergehende Unterschreitung (z. B. wegen kurzfristigen Ausscheidens von Mitarbeitenden) ist unbeachtlich, wenn die Mindestzahl regelmäßig erreicht wird. Mit der h. M.[4] zur alten Rechtsprechung ist davon auszugehen, dass dieses Kriterium erfüllt ist, wenn der Schwellenwert über einen Zeitraum von einem Jahr erreicht wurde oder bei einer vorausschauenden Betrachtung erreicht werden wird.[5]

1 Däubler, Rn. 136h
2 § 20 Abs. 2 KDO lautet: *„Sind mit der automatisierten Datenerhebung, -verarbeitung oder -nutzung mehr als zehn Personen befasst …"*. Damit war eine Angleichung an das BDSG, § 38 Abs. 1, erfolgt, die jedoch durch das 2. Datenschutzanpassungs- und Umsetzungsgesetz vom 28.6.2019 obsolet wurde, weil damit vom Bundestag der Grenzwert auf 20 Personen erhöht wurde.
3 Der staatliche Gesetzgeber hat sich an dieser Stelle genau andersherum entschieden und orientiert den Grenzwert jetzt an den Personen, die mit *automatisierter* Datenverarbeitung beschäftigt sind, vgl. § 38 Abs. 1 BDSG.
4 Simitis in Simitis, § 4f BDSG a. F. Rn. 20; Gola/Schomerus, § 4 BDSG a. F. Rn. 11; DKWW, § 4f Rn.18
5 Jaspers/Reif in Heidelberger Kommentar, Art. 37 Rn. 27

§ 36 Abs. 1 lit. b dürfte für Einrichtungen von Kirche und Caritas selten einschlägig sein. Aufgaben, die eine umfangreiche, regelmäßige und systematische Überwachung aufgrund ihres Zwecks, ihrer Art oder ihres Umfangs erforderlich machen, sind vor allem solche, die mit Profiling-Maßnahmen[1] oder Scoring-Maßnahmen[2] einhergehen und die Kerntätigkeit der Einrichtung darstellen. Denkbar sind solche Voraussetzungen vor allem bei Fundraising-Einrichtungen. 480

Gem. § 36 Abs. 2 lit. b KDG sind solche Einrichtungen zur Benennung eines betrieblichen Datenschutzbeauftragten, unabhängig von der Zahl der bei ihnen Beschäftigten, verpflichtet, deren Kerntätigkeit in der Verarbeitung besonderer Kategorien personenbezogener Daten gem. § 4 Nr. 2 KDG besteht. Eine Kerntätigkeit liegt vor, wenn es sich um die Haupttätigkeit der Einrichtung handelt. Das heißt, die wesentliche Aufgabe der Einrichtungsziele ist nicht zu erreichen, ohne dass personenbezogene Daten besonderer Kategorie verarbeitet werden.[3] Dies ist regelmäßig in Gesundheits- und Pflegeeinrichtungen sowie in Beratungsstellen der Fall. Damit werden Caritaseinrichtungen nur in Ausnahmefällen von der Bestellung eines betrieblichen Datenschutzbeauftragten befreit sein. 485

## 3.1 Benennung

Entgegen den staatlichen Regelungen hat die Benennung gem. § 36 Abs. 1 KDG **schriftlich** zu erfolgen. Die Schriftform ist konstitutiv. Ohne eine schriftliche Benennung ist diese unwirksam.[4] 490

Eine Bestellung gegen den Willen des Arbeitnehmers ist nicht möglich, da sowohl die Bestellung als auch die Abberufung als betrieblicher Datenschutzbeauftragter eine **Änderung des Arbeitsvertrages** bedeuten, die vom Arbeitnehmer angenommen werden muss.[5] Aus diesem Grunde ist aus Nachweisgründen anzuraten, die Bestellungsurkunde vom betrieblichen Datenschutzbeauftragten mit unterschreiben zu lassen.[6] Bei der Bestellung eines externen betrieblichen Datenschutzbeauftragten wird ein Dienstvertrag abgeschlossen, der von beiden Vertragsparteien zu unterschreiben ist. 495

Nur bei der Bestellung eines Beschäftigten zum betrieblichen Datenschutzbeauftragten enthält das KDG Regeln für die **Dauer der Benennung.** Gem. § 36 Abs. 5 Satz 2 KDG, der auf die Regelungen des § 42 Abs. 1 Satz 1 500

1 Paal in Paal/Pauly, Art. 37 Rn. 8
2 Klug, ZD 2016, 315; Dammann, ZD 2016, 307
3 Art. 29 Gruppe WP 243 S. 8
4 Praxishilfen zum KDG, herausgegeben von der Konferenz der Diözesandatenschutzbeauftragten, einzusehen auf den Homepages der Diözesandatenschutzbeauftragten
5 BAG, Urteil vom 13.3.2007, 9 AZR 612/05, DB 2007, 1198, 1200
6 Dies gilt gleichermaßen für das staatliche Recht außerhalb des Anwendungsbereiches des KDG; Paal in Paal/Pauly, Art. 37 Rn. 16, Drewes in Simitis, Art. 37 Rn. 52

HS 2 KDG und § 42 Abs. 1 Satz 2 KDG verweist, darf eine Bestellung auf mindestens vier und höchstens acht Jahre befristet werden. Erneute Bestellungen nach Ablauf der jeweiligen Frist sind möglich. Darüber hinaus wird in § 37 Abs. 4 KDG dem Beschäftigten, der zum betrieblichen Datenschutzbeauftragten bestellt wird, ein Kündigungsschutz zugesprochen, der dem von Mitgliedern der MAV entspricht. Das heißt, das Arbeitsverhältnis kann innerhalb der Bestellungszeit und ein Jahr danach nur aus wichtigem Grund gekündigt werden.

505 Eine **Abberufung** des betrieblichen Datenschutzbeauftragten unter Beibehaltung seines Arbeitsverhältnisses im Übrigen ist nicht möglich, da ein solches Verfahren eine unzulässige Teilkündigung darstellte,[1] oder aber als Änderungskündigung ebenfalls dem Kündigungsverbot des § 37 Abs. 4 KDG unterfiele. Festzustellen ist aber auch, dass eine dem § 20 Abs. 8 KDO entsprechende Regelung im KDG fehlt. Nach dieser Vorschrift, die auf § 16 KDO verwies, musste der Verantwortliche auf Antrag des Beauftragten die Bestellung zurücknehmen. Auch der betriebliche Datenschutzbeauftragte ist, weil mit seiner Bestellung arbeitsvertragliche Pflichten festgeschrieben worden sind, daran gehindert, seine Tätigkeit als betrieblicher Datenschutzbeauftragter einfach aufzugeben, wenn eine entsprechende Öffnung im Arbeitsvertrag fehlt. Gleichwohl ist es beiden Vertragsparteien nicht verwehrt, einen einvernehmlichen Aufhebungs- oder Änderungsvertrag zu vereinbaren.

### 3.2 Veröffentlichung der Kontaktdaten

510 § 36 Abs. 4 KDG verlangt die Veröffentlichung der Kontaktdaten des betrieblichen Datenschutzbeauftragten. Im Gegensatz zu § 15 Abs. 1 lit. a KDG ist hier ausdrücklich nicht die Verpflichtung benannt, den Namen zusätzlich oder im Rahmen mit den Kontaktdaten anzugeben. Erforderlich ist die Bekanntgabe solcher Kontaktdaten, die es ermöglichen, den betrieblichen Datenschutzbeauftragten kurzfristig auf einfachem Weg zu erreichen. Eine Angabe des Namens ist darüber hinaus nicht erforderlich.[2]

515 Obwohl über die Art der Veröffentlichung im Gesetz keine Aussage getroffen ist, ist es nach dem Sinn und Zweck erforderlich, eine Veröffentlichung auf dem Medium anzubringen, mit dem die betroffene Person in Kontakt kommt. Unterhält der Verantwortliche eine Internetpräsens, ist eine permanente Mittelung dort an einer leicht auffindbaren Stelle ausreichend. Bei Verwendung von Briefpost kann ein entsprechender Hinweis auf die Internetseite erfolgen.

520 Gleichzeitig legt die Vorschrift fest, die Benennung des betrieblichen Datenschutzbeauftragten der Datenschutzaufsicht mitzuteilen. Damit soll

1 Preis, Erfurter Kommentar, 18. Auflage 2018, § 611a BGB Rn. 377
2 Art. 29 Gruppe WO 243 S. 15

es der Datenschutzaufsicht ermöglicht werden zu überprüfen, welche Einrichtungen der Verpflichtung zur Bestellung nachgekommen sind. Die Formulierung in Abs. 4 Satz 2, die nach Abs. 1 benannten betrieblichen Datenschutzbeauftragten der Datenschutzaufsicht anzuzeigen, ist vor dem Hintergrund des Zwecks der Vorschrift als Redaktionsversehen zu betrachten. Richtigerweise ist hier der Verweis auf § 3 Abs. 1 KDG zu unterstellen.

**Nicht zu betrieblichen Datenschutzbeauftragten** „sollen" nach § 36 Abs. 7 KDG diejenigen bestellt werden, die mit der Leitung der Datenverarbeitung betraut sind oder denen die Leitung der kirchlichen Einrichtung obliegt. Das bedeutet, dass dieser Personenkreis grundsätzlich von der Benennung ausgenommen ist. Soweit die Formulierung dazu führt, das „soll" als unverbindlich zu betrachten, ist die Verwendung unglücklich. Bei einer „Soll"-Vorschrift ist der Verantwortliche im Regelfall zum Tätigwerden strikt verpflichtet. Ansonsten muss er nachweisen, dass ein atypischer Fall vorliegt. Es müssen konkrete, nicht vom Verantwortlichen selbst zu vertretende Gründe für das Abweichen von der Norm sprechen.[1] Um von einem atypischen Fall sprechen zu können, muss die Abweichung so bedeutend sein, dass das Gewicht der für die Regelentscheidung maßgeblichen Gründe beseitigt wird.[2] 525

**Mitglieder der MAV** können zu betrieblichen Datenschutzbeauftragten bestellt werden. Dies ergibt sich bereits aus den gleichgerichteten Interessen des Datenschutzbeauftragten und des MAV-Mitgliedes, die u. a. in der konsequenten Umsetzung des Datenschutzgesetzes bestehen.[3] Wollte man Mitarbeitervertreter generell als ungeeignet ansehen, würde dies auf eine Benachteiligung gegenüber anderen Arbeitnehmern hinauslaufen.[4] Seit einer Entscheidung des BAG im Jahr 2011 ist diese Frage für Betriebsratsmitglieder geklärt.[5] 530

In diesem Zusammenhang ist umstritten, ob sich die Zuständigkeit des betrieblichen Datenschutzbeauftragten auch auf die MAV bzw. deren Büro erstreckt, oder ob die MAV als eigener Verantwortlicher i. S. v. § 4 Nr. 9 KDG zu betrachten ist.[6] Während das BAG[7] die erste Frage verneint hat, hat der Landesbeauftragte für Datenschutz Baden-Württemberg[8] die zweite Frage bejaht. Nach hier vertretener Meinung sind beide Ansichten abzulehnen. 535

1 Kopp/Ramsauer, VwVfG 16. Auflage 2015, § 40 Rn. 63
2 Sachs in Stelkens/Bonk/Sachs, VwVfG 8. Auflage 2014, § 40 Rn. 27
3 Für den Betriebsrat: Bommer ZD, 2015, 123; Däubler, Rn. 596; eher ablehnend BfDI, Info 4 „Die Datenschutzbeauftragten in Behörden und Betrieb" S. 16
4 DKWW, § 4f Rn. 32; a. A. Bergmann/Möhrle/Herb, § 4f Rn. 105
5 BAG, Urteil vom 23.3.2011, 10 AZR 562/09
6 Dazu ausführlich Ullrich, ZAT 2019, Heft 3
7 BAG, Beschluss vom 11.11.1997, 1 ABR 21/97
8 LfDI Baden-Württemberg 34. TB 2018 S. 37

Zunächst hatte die Rechtsprechung des BAG die bis dahin umstrittene Frage zwar de facto beendet. Jedoch wurde diese Entscheidung schon nach ihrem Erscheinen als europarechtswidrig kritisiert.[1] Das BAG konnte sich seinerzeit wegen einer entsprechenden Regelung in § 1 Abs. 3 BDSG a. F. darauf berufen, dass das Betriebsverfassungsgesetz als speziellere Norm dem BDSG vorgehe. Seit in Krafttreten der DSGVO ist aber aufgrund der unmittelbaren Wirkung gem. Art. 288 Abs. 2 AEUV das Verhältnis der Rechtsnormen umgekehrt worden. Durch nationalstaatliche Gesetze dürfen nur solche Regelungen erlassen werden, für die die DSGVO eine Öffnung vorsieht.

### 3.3 Weitergeltung von Altbestellungen

Soweit die Bestellung eines betrieblichen Datenschutzbeauftragten auf der Grundlage der KDO wirksam vorgenommen worden ist, ist eine Benennung nach dem KDG nur wegen der neuen Rechtsgrundlage nicht erforderlich, da die Rechtsstellung des betrieblichen Datenschutzbeauftragten dadurch nicht verändert wird.[2]

### 3.4 Erreichbarkeit

§ 36 KDG lässt zu, für mehrere kirchliche Stellen unter Berücksichtigung ihrer Organisationsstruktur und Größe einen betrieblichen Datenschutzbeauftragten zu bestimmen. Diese Regelung ähnelt der in Art. 37 Abs. 2 DSGVO. In der europäischen Regelung ist die Verpflichtung enthalten, dass der Datenschutzbeauftragte von jeder Niederlassung leicht erreichbar sein muss. Dieser ausdrückliche Hinweis fehlt im KDG. Dafür gesteht das KDG unter § 37 Abs. 3 jedem Betroffenen zu, sich jederzeit und unmittelbar an den betrieblichen Datenschutzbeauftragten wenden zu können.

Im Hinblick auf die „leichte Erreichbarkeit" ist eine **persönliche Erreichbarkeit** zu verstehen.[3] 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.[4] Das gleiche gilt im Hinblick auf die in Art. 38 Abs. 5 DSGVO festgeschriebene Wahrung der Geheimhaltung und Vertraulichkeit des betrieblichen Datenschutzbeauftragten, auch diese Forderung macht eine persönliche Anwesenheit erforderlich.[5]

1 Aßmus, ZD 2011, 27; Ehmann, CR 1998, 332; Simitis/Simitis, BDSG a. F., § 4g Rn. 42
2 Datenschutzkonferenz Kurzpapier 12 S. 3; Jaspers/Reif in Heidelberger Kommentar, Art. 37 Rn. 29
3 Sydow, DSGVO Art. 37 Rn. 96; Paal/Pauly, DSGVO Art. 37 Rn. 10; Jaspers/Reif in Heidelberger Kommentar Art. 37 Rn. 32
4 Jaspers/Reif, Art. 37 Rn. 32
5 Sydow, Art. 37 Rn. 97

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, müssen der Betroffene oder der Verantwortliche diesen innerhalb eines achtstündigen Arbeitstages erreichen können. Dies stellt eine maximale Grenze dar, die Hin- und Rückfahrt inkludiert.[1] Die Erfüllung dieser Forderung erscheint insbesondere dann fraglich, wenn in einem Bistum für alle Pfarreien oder in einem diözesanen Caritasverband für alle Caritasdienststellen nur ein gemeinsamer Betrieblicher Datenschutzbeauftragter bestellt ist. 560

## 4. Informationspflichten

Im Dritten Kapitel des KDG werden Informationspflichten des Verantwortlichen und Rechte der betroffenen Personen geregelt. Während die Grundsätze der Verarbeitung personenbezogener Daten in § 7 KDG geregelt sind, konkretisieren die §§ 14 ff. KDG die dort festgeschriebenen Grundsätze durch die Rechte der betroffenen Personen. Die Rechte der betroffenen Personen sind im deutschen Recht bereits durch das grundlegende Volkszählungsurteil des BVerfG[2] festgelegt worden, wenn dort gefordert wird, dass jeder, der von der Verarbeitung personenbezogener Daten betroffen ist, die Möglichkeit haben muss zu erfahren, wer, was, wann und bei welcher Gelegenheit über ihn weiß. Genau das bedeutet Transparenz, wie sie in § 14 KDG postuliert wird. Ein solches Recht wird durch Art. 8 Abs. 2 Satz 2 GRCh vorgegeben. Voraussetzung für die Wahrnehmung des Rechtes auf informationelle Selbstbestimmung ist, dass der Betroffene über die Erhebung personenbezogener Daten, über die Art und Weise ihrer Verarbeitung und die Zwecke der Nutzung verständlich aufgeklärt worden ist.[3] 565

§ 14 KDG regelt dabei zunächst Verfahrensfragen, die für die folgenden Vorschriften §§ 15 - 21 KDG gleichsam vor die Klammer gezogen werden,[4] weil sie für die folgenden Vorschiften gelten. 570

Eine Legaldefinition für die in § 14 KDG genannten Begriffe „angemessene Frist“, „präzise“, „transparente“, „verständliche“ und „leicht zugängliche Form“, die die Art und Weise der Information beschreiben, findet sich nicht. So ist festzustellen, dass deren Bedeutung sich teilweise überlagert bzw. die Begriffe in Teilen widersprüchlich erscheinen. 575

1 So auch Jaspers/Reif, Art. 37 Rn. 32 für die europäische Gesetzesregelung
2 BVerfGE 65, 44
3 Greve in Sydow, Art. 12 Rn. 3
4 Schwartmann/Schneider in Heidelberger Kommentar, Art. 12 Rn. 14

### 4.1 Angemessene Frist

580 § 14 Abs. 1 Satz 1 KDG verpflichtet den Verantwortlichen, geeignete Maßnahmen zu ergreifen, um der betroffenen Person alle Informationen gem. §§ 15 u. 16 KDG und alle Mitteilungen gem. §§ 17 – 24 und 34 KDG *innerhalb angemessener Frist* zur Verfügung stellen zu können. Diese Formulierung ist zumindest unglücklich, da gem. § 14 Abs. 3 KDG die Informationen nach den §§ 17 – 24 KDG *unverzüglich* zu erfolgen haben und § 15 Abs. 1 KDG verlangt, dass die Information bereits im *Zeitpunkt der Erhebung* erfolgt.

585 Somit ist durch die Formulierung *innerhalb angemessener Frist* keine abweichende oder sogar weitergehende Frist geschaffen, sondern diese kann nur als gleichbedeutend mit *unverzüglich* verstanden werden, soweit das KDG nicht, wie in § 15, eine kürzere Frist bestimmt. Der Rechtsbegriff *unverzüglich* ist in § 121 BGB als „ohne schuldhaftes Zögern" legal definiert.[1] Damit unterscheidet sich die Zeitbestimmung von dem Begriff *„sofort"*, der als *„so schnell wie objektiv möglich"* definiert ist. Die Information muss demnach innerhalb einer nach den Umständen des Einzelfalls zu bestimmenden Prüfungs- und Überlegungsfrist[2] erfolgen.

590 Soweit in § 14 Abs. 3 KDG „in jedem Fall aber innerhalb eines Monats" formuliert ist, ist darin keine Regelfrist zu sehen, sondern nur eine gerade noch zulässige Höchstfrist für Standardinformationen.[3] Im Ausnahmefall kann der Verantwortliche im Falle besonders komplexer Informationen und Auskünfte die Frist selber um zwei weitere Monate verlängern, wenn er der betroffenen Person innerhalb eines Monats nach Eingang des Antrages begründet, auf welchen Umständen die Fristverlängerung beruht. Die betroffene Person hat dann die Möglichkeit, die Begründung für die Fristverlängerung durch die kirchliche Datenschutzaufsicht überprüfen zu lassen. In jedem Fall ist eine weitere Verlängerung der Frist zur Informationserteilung ausgeschlossen.

### 4.2 Verständlichkeit

959 Die Anforderungen, die Information in präziser und leicht zugänglicher Form in verständlicher Sprache darzustellen, verlangt dem Verantwortlichen erhebliche Anstrengungen ab, da die Erfüllung einer Anforderung nicht zulasten der anderen gehen darf. So darf die Einfachheit der Sprache nicht die Präzision beeinträchtigen. Gleichzeitig darf Präzision aber auch

1 Da es sich bei dem KDG um eine deutsche Rechtsnorm handelt, ist auf die Frage, ob der in der DSGVO verwendete europarechtliche Begriff „unverzüglich" durch eine deutsche Rechtsnorm legal definiert werden kann, nicht einzugehen. Siehe für die DSGVO Heidelberger Kommentar, Art. 12 Rn. 50; demgegenüber Paal/Pauly, Art. 12 Rn. 53.
2 Ellenberger in Palandt, § 121, Rn. 3
3 Dix in Simitis, Art. 12 Rn. 25

keinen Umfang erreichen, der zu Ermüdung oder Abschreckung führt und somit nicht mehr verständlich ist.[1] Präzise ist eine Information, wenn sie einen hinreichenden Grad an Genauigkeit aufweist.[2] Die Information ist also vollständig darzustellen, aber dabei „auf den Punkt" zu bringen, d. h. auf den für die betroffene Person relevanten Kern zu reduzieren.[3]

Bei der Verständlichkeit ist der **Empfängerhorizont** zu berücksichtigen. 600
Die Information muss deshalb für den jeweiligen Adressatenkreis aus sich heraus verständlich sein.[4] Da die Fähigkeiten des Adressatenkreises häufig nicht bekannt sein werden, empfiehlt es sich, auf einen eher unterdurchschnittlichen Anwender abzustellen.[5] Da wie bereits ausgeführt eine umfangreiche und detaillierte Darstellung zwar sehr präzise sein kann, häufig aber dazu führen wird, dass der durchschnittliche Nutzer den Ausführungen nicht mehr folgen kann, ist eine mehrschichtige Information eine Möglichkeit, dieses Spannungsverhältnis aufzulösen.[6] Die betroffene Person erhält eine Information, innerhalb derer sie die Möglichkeit erhält, für bestimmte Begriffe oder Verfahrensbeschreibungen auf weitere Informationen zugreifen zu können. Eine solche Darstellung ist im Rahmen einer elektronischen Information einfacher zu gestalten, da durch „anklicken" bestimmter Textpassagen auf eine tiefere Ebene zugegriffen werden kann.

Dabei ist eine **„einfache Sprache"** zu verwenden. Eine Definition für „ein- 605
fache Sprache" besteht nicht. Zwar bestehen in Deutschland zum Teil verbindliche Regeln für „einfache" oder „leichte" Sprache,[7] diese sind jedoch nicht zwingend für die Informationspflicht anzuwenden, können aber eine Orientierung geben.[8] Auch hierbei ist nicht vom Durchschnittsnutzer auszugehen, sondern die Sprache muss auch Personen mit deutlich geringerem Bildungsniveau erreichen.[9] Fremdwörter sollten nur verwendet werden, wenn es sich nicht vermeiden lässt. In diesem Fall sind die Fremdwörter möglichst zu erklären. Darüber hinaus sollten Sätze möglichst kurz gebildet werden und nicht mehr als ein Komma enthalten. Zu verwenden ist mithin eine Alltagssprache[10], wie sie regelmäßig in Printerzeugnissen der Boulevardpresse Verwendung findet.

1 Dix, Art. 12 Rn. 12
2 Schwartmann/Schneider in Heidelberger Kommentar, Art. 12 Rn. 24
3 Heckmann/Paschke in Ehmann/Selmayr, DSGVO Rn. 12
4 Schwartmann/Schneider, Art. 12 Rn. 25
5 Heckmann/Paschke, DSGVO Rn. 13
6 Art. 29 Datenschutzgruppe WP 260 S. 17; Paal in Paal/Pauly, Art. 12 Rn. 31
7 Vgl. Ratgeber leichte Sprache, www.bmas.de
8 Dix in Simitis, Art. 12 Rn. 14
9 Franck in Gola, DSGVO, Art. 12 Rn. 22.
10 Härting, DSGVO S. 20

610 Vor den genannten Ausführungen wird deutlich, dass die Einhaltung von Präzision, einfacher Zugänglichkeit und Verständlichkeit bereits zu Transparenz führen. Deshalb kommt diesem Begriff innerhalb der Regelung keine eigenständige, darüberhinausgehende Bedeutung zu.[1] Transparenz stellt gleichsam den Oberbegriff dar.

615 Die Informationspflichten aus dem Transparenzgebot sind auch gegenüber **Minderjährigen**[2] zu achten. In der Praxis bedeutet dies u. a., dass Kinder auch dann ein Recht auf Information gem. §§ 14 ff. KDG haben, wenn die Sorgeberechtigten für sie eine Einwilligung abgegeben haben. Minderjährige haben im Rahmen der gesamten Interaktion mit dem Verantwortlichen ein permanentes Recht auf Transparenz.[3]

620 Verantwortliche, die sich der Tatsache bewusst sind oder bewusst sein müssen, dass von der Verarbeitung personenbezogener Daten schutzbedürftigen Menschen betroffen sind, müssen bei Art und Inhalt der Information die besondere Schutzbedürftigkeit berücksichtigen. Das trifft z. B. Menschen mit Behinderung in einer Werkstatt für solche Menschen, die ggf. Schwierigkeiten haben, Zugang zu Informationen zu erlangen.[4]

### 4.3 Formerfordernis

625 Im Hinblick auf die Form der Information ist eine Gleichrangigkeit zwischen schriftlicher, elektronischer oder anderer Form vorgesehen. Da eine Definition im KDG nicht benannt ist, ist auf die Legaldefinition der jeweiligen Begriffe in den §§ 126 ff. BGB abzustellen. Aufgrund der Gleichrangigkeit ist auf die Unterscheidungen im Einzelnen an dieser Stelle nicht einzugehen.

630 Eine Übermittlung in anderer Form ist auch dann gegeben, wenn die Informationen auf einer öffentlich zugänglichen Homepage zur Verfügung stehen.[5] Die Informationen dürfen aber auf der Homepage nicht versteckt platziert sein. Es sind vielmehr die gleichen Grundsätze zu beachten, die auch bislang schon für das Impressum und die Datenschutzerklärung bestanden und bei der Einbeziehung von AGB bei Vertragsabschluss gelten.[6]

1 Paal in Paal/Pauly, Art. 12 Rn. 29
2 In der DSGVO wird der Begriff „Kinder“ verwendet. Nach dem Übereinkommen der Vereinten Nationen über die Rechte des Kindes ist darunter eine Person unter 18 Jahren zu verstehen. Es besteht also kein inhaltlicher Unterschied zwischen beiden Formulierungen.
3 Artikel 29 Gruppe WP 260 S. 12
4 Artikel 29 Gruppe WP 260 S. 12
5 Erwägungsgrund 58, Ehmann/Selmayr, Art. 12 DS-GVO Rn. 22
6 Wybitul, EU Datenschutzgrundverordnung 1. Auflage 2017, Art. 12 - 15 Rn. 12; Konferenz der Diözesandatenschutzbeauftragten Praxishilfe Nr. 6 „Betroffenenrechte“ S. 4

Lediglich für die mündliche Information sieht das Gesetz vor, dass die betroffene Person, die eine solche Information verlangt, diese nur erteilt bekommen darf, wenn die Identität der betroffenen Person in anderer Form nachgewiesen wurde. In anderer Form heißt zunächst, dass die Identität nicht mündlich belegt werden kann, sonst aber jede beliebige Möglichkeit zur Verfügung steht.[1] Dazu zählen u. a. Identitätsnachweis durch Pass, Personalausweis, elektronischen Identitätsnachweis, Identitätsbestätigungsdienst u. a.[2] Die Verpflichtung, sich der Identität der betroffenen Person hinreichend zu versichern, trifft aber nicht bei allgemeinen Datenschutzinformationen gem. §§ 14 und 15 KDG zu, da diese Informationen auch zukünftigen Nutzern zugänglich gemacht werden müssen.[3] 635

Die Auskunft hat kostenlos zu erfolgen (§ 12 Abs. 5 KDG). Eine Ausnahme ist nur dann gegeben, wenn eine betroffene Person offenkundig unbegründete Anträge stellt oder das Informationsrecht durch exzessive Antragstellung überstrapaziert wird. Offenkundig unbegründet ist ein Antrag, wenn die Voraussetzungen des Anspruchs ganz offensichtlich nicht erfüllt sind und dies jedem verständigen Antragsteller bewusst sein muss.[4] Das wird bei einer Erst-Antragsstellung in den seltensten Fällen vorkommen.[5] Ein solcher Fall könnte gegeben sein, wenn Dritte ein Auskunftsrecht für betroffene Personen fordern, ohne entsprechend beauftragt zu sein.[6] 640

Eine exzessive Antragstellung liegt nicht bereits dann vor, wenn das Auskunftsrecht in regelmäßigen Abständen verlangt wird. Die Abstände müssen jedoch „angemessen" sein.[7] Eine solche Angemessenheit liegt definitiv nicht vor, wenn wiederholte Anträge innerhalb der Frist gestellt werden, die der Gesetzgeber für die Beantwortung der Auskunft in § 14 Abs. 3 KDG eingeräumt hat. Darüber hinaus ist von einer exzessiven Antragstellung auszugehen, wenn nahezu wort- oder inhaltsgleiche Anträge ohne tragfähige Begründung häufig wiederholt werden.[8] Wann eine exzessive Antragstellung vorliegt, hängt somit vom Einzelfall ab. Regelmäßig wird sie aber bei einer erneuten Antragstellung vor Ablauf von drei Monaten anzunehmen sein[9], während bei einer erneuten Antragstellung nach Ablauf eines Jahres regelmäßig von einer berechtigten Antragstellung auszugehen sein wird.[10] 645

1 Schwartmann/Schneider in Heidelberger Kommentar, Art. 12 Rn. 37
2 Beispiele aus Greve in Sydow, Art. 12 Rn. 19
3 Artikel 29 Gruppe WP 260 S. 14
4 Heckmann/Paschke in Ehmann/Selmayr, DSGVO Art. 12 Rn. 43; Greve in Sydow, Europäische Datenschutzgrundverordnung Art. 12, Rn. 26
5 Dix in Simitis, Art. 12 Rn. 32; Greve in Sydow, Art. 12 Rn. 26
6 Heckmann/Paschke in Ehmann/Selmayr, DSGVO Art. 12 Rn. 43
7 Erwägungsgrund 63 S. 1
8 Greve in Sydow, Art. 12, Rn. 26, Paal in Paal/Pauly, Art. 12 Rn. 64
9 Gola, DSGVO Art. 15, Rn. 35
10 Mehr als ein Jahr: Schwartmann/Klein, Heidelberger Kommentar, Art. 15 Rn. 18

## 5. Betroffenenrechte

650 Für einen fairen und transparenten Umgang mit der Verarbeitung personenbezogener Daten ist es erforderlich, dass jede betroffene Person die Möglichkeit bekommt, sich der Verarbeitung bewusst zu werden und deren Rechtmäßigkeit überprüfen zu können.[1] Jede betroffene Person hat Anspruch darauf, vom Verantwortlichen Auskunft darüber zu erhalten, ob und ggf. welche personenbezogenen Daten dieser vom Betroffenen verarbeitet.

655 Der Anspruch ist somit zweigeteilt. Zunächst ist vom Verantwortlichen zu prüfen, ob überhaupt personenbezogene Daten verarbeitet werden. Ist dies nicht der Fall, darf sich der Verantwortliche aber nicht in Untätigkeit üben, weil „ihn die Sache nichts angeht". Er ist vielmehr durch § 17 KDG verpflichtet, eine entsprechende Negativauskunft an die betroffene Person zu richten.[2] Eine solche Negativauskunft ist auch in den Fällen zu erteilen, in denen Daten durch Anonymisierung den Personenbezug verloren haben.[3] Obwohl § 17 KDG zwei Ansprüche formuliert, sind an den Inhalt des Auskunftsanspruchs keine zu hohen Anforderungen zu stellen. So dürfte die Frage des Betroffenen, „ob" personenbezogene Daten über ihn verarbeitet werden, regelmäßig auch darauf gerichtet sein zu erfahren, „welche" personenbezogenen Daten verarbeitet werden[4] und umgekehrt.

660 Liegt eine Verarbeitung personenbezogener Daten vor, hat die betroffene Person Anspruch auf Auskunft und Information über alle konkret zu ihr verarbeiteten personenbezogenen Daten. Darüber hinaus hat die betroffene Person in diesem Fall Anspruch auf die Informationen nach § 17 Abs. 1 lit. a bis h. Inhalt des Auskunftsanspruchs ist also die Auskunft über die konkret verarbeiteten personenbezogenen Daten. Dabei ist nur zu entscheiden, ob ein Personenbezug vorliegt und ob die Daten Gegenstand einer Verarbeitung i. S. v. § 4 Nr. 3 sind.[5]

665 Nach § 17 Abs. 3 KDG stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Diese erste Kopie ist kostenlos, was sich aus dem nachfolgenden Satz ergibt, der ausdrücklich weitere Kopien von der Erstattung eines angemessenen Entgeltes abhängig macht. Bei einer elektronischen Beantragung sind die Kopien auch elektronisch zur Verfügung zu stellen. Zu beachten ist auch hierbei die Verschlüsselung der personenbezogenen Daten als Voraussetzung der elektronischen Übersendung. § 17 Abs. 3 KDG gibt der betroffenen Person über den in Abs. 1 hinaus genannten Anspruch auf die

1 Erwägungsgründe 60 und 63
2 Dix in Simitis, Art. 15 Rn. 12
3 Paal in Paal/Pauly, Art. 15 Rn. 19
4 Dix in Simitis, Art. 15 Rn. 14; a. A. Paal, Art. 15 Rn. 21
5 Engler/Quiel, NJW 2019, 2201

Benennung der verarbeiteten personenbezogenen Daten einen Anspruch darauf, diese so zu erhalten, wie sie beim Verantwortlichen vorliegen. Der Betroffene erfährt dadurch auch, auf welche Art und Weise seine personenbezogenen Daten verarbeitet werden, was ihm eine zusätzliche Überprüfung ermöglicht.[1]

Das Recht auf eine Kopie ist weit auszulegen. Verweigert werden kann eine solche dann, wenn darin Daten von Dritten enthalten sind, oder wenn mit der Kopie Urheber- oder Geschäftsgeheimnisse betroffen sind und eine Güterabwägung zu dem Schluss kommt, dass diese überwiegen.[2] Das Recht auf eine Kopie erfasst aber auch solche Daten, die der Betroffene bereits kennt, oder solche, die nur zu internen Zwecken verwendet werden.[3] Die entgegenstehende Auffassung ist abzulehnen, da eine pauschale Ausnahme, wie sie § 16 Abs. 5 lit. a formuliert, in § 17 fehlt. 670

## 6. Videoüberwachung

Eine ausdrückliche Regelung zur Videoüberwachung findet sich in der DSGVO nicht. Jedoch wird die Rechtmäßigkeit der Verarbeitung von Daten in Art. 6 DSGVO geregelt. Dessen Abs. 1 lit. e und Abs. 3 beschränken den Regelungsspielraum der Mitgliedstaaten auf die Fälle, in denen es sich bei der Videoüberwachung um die Wahrnehmung von Aufgaben im öffentlichen Interesse oder der Ausübung öffentlicher Gewalt handelt. Vor diesem Hintergrund erscheint die Zulässigkeit des § 4 BDSG europarechtlich fraglich, da die dortigen Vorschriften den von der DSGVO eröffneten Regelungsbereich deutlich überschreiten.[4] Die Zulässigkeit von Videoaufnahmen im außerkirchlichen Bereich wird deshalb zukünftig nach Art. 6 Abs. 1 lit. f DSGVO zu bestimmen sein.[5] 675

Der **kirchliche Gesetzgeber** war hingegen durch die Regelungen der DSGVO nicht gehindert, ausdrückliche Regelungen zur Videoüberwachung zu etablieren. In § 52 KDG finden sich Vorschiften, die die Zulässigkeit von Videoaufnahmen im Bereich öffentlich zugänglicher Räume regeln. Mit dieser Vorschrift übernimmt das KDG die Regelungen, die sich bislang in § 5a KDO befanden. Lediglich die Terminologie wurde an den neuen Gesetzestext angepasst. 680

Im KDG wird der Begriff „Videoüberwachung“ legal definiert, als Beobachtung mit „optisch-elektronischen Einrichtungen“. Darunter fallen alle Geräte, die zu einer Bildaufzeichnung oder Überwachung eingesetzt 685

1 Ebd.
2 Ebd.
3 Ebd.
4 Kühling/Buchner, § 4 BDSG Rn. 2
5 Lachenmann, ZD 2017, 407, 409

werden können. Das sind nicht nur klassische Videogeräte[1], sondern z. B. auch Dash-Cams, Kameras für die Überwachung der Einlasskontrolle, Drohnen usw.[2] Dabei ist es egal, ob diese Geräte mobil oder fest installiert sind[3] und ob sie digital oder analog arbeiten[4].

690 Der Begriff „Beobachtung" macht zum einen deutlich, dass es auf eine Aufzeichnung der Bilder nicht ankommt und somit auch Monitoring-Systeme unter die Vorschrift fallen. Das sind solche Systeme, bei denen die Bilder direkt auf einen Bildschirm übertragen werden, der von einer Überwachungsperson beobachtet wird[5]. Zum anderen wird nur die automatisierte Verarbeitung von personenbezogenen Daten durch die Vorschrift erfasst. Das Vorliegen einer Datenverarbeitung ist demnach grundsätzlich Voraussetzung für die Anwendbarkeit. Bei Kameraattrappen geschieht das nicht.

695 Das LG Essen[6] hat es aber genügen lassen, dass durch eine Kameraattrappe ein Überwachungsdruck für Betroffene entsteht, der deren Persönlichkeitsrecht in gleicher Weise einschränkt wie eine tatsächliche Kamera. Diese Sichtweise erscheint auch folgerichtig vor dem Hintergrund, dass das BAG einen unzulässigen Überwachungsdruck auch für den Fall anerkennt, dass eine Kamera angebracht ist, die nur zeitweise aufzeichnet, Mitarbeitende aber nicht wissen, wann Aufzeichnungen stattfinden. Wenn also eine Kamera, die möglicherweise den ganzen Tag ausgeschaltet ist, einen Überwachungsdruck erzeugt, muss das in gleicher Weise auf eine Attrappe zutreffen.[7]

700 Aus diesem Grund ist auch entgegen der Rechtsauffassung des LAG Mecklenburg-Vorpommern[8] ein Mitbestimmungsrecht der MAV gem. § 36 Abs. 1 Nr. 9 MAVO bei der Installation von Kameraattrappen begründet. Dieses Mitbestimmungsrecht ist u. a. darauf gerichtet, den Dienstnehmer vor unverhältnismäßigen Beeinträchtigungen seines Persönlichkeitsrechts zu schützen. Das Persönlichkeitsrecht des Dienstnehmers ist aber nur dann nicht beeinträchtigt, wenn er darum weiß, dass es sich bei der entsprechenden Kamera um eine Attrappe handelt. Andernfalls wird er sich aufgrund der Unsicherheit, ob er gefilmt wird oder nicht, anders und damit nicht frei verhalten und die Attrappe wird so eine ordnungsverhaltenssteuernde Wirkung entfalten.[9]

1 Scholz in Simitis, § 6b Rn. 38
2 BeckOK Datenschutzrecht, Wolff/Brink Rn. 5
3 Kühling/Buchner, § 4 BDSG Rn. 8
4 Scholz in Simitis, § 6b Rn. 70
5 Wedde in DKWW, § 6b Rn. 13
6 LG Essen, Urteil vom 30.1.2019, 12 O 62/18; ebs. Däubler, Rn. 299
7 BAG, Urteil vom 7.10.1987, 5 AZR 116/86; Däubler, Rn. 308 m.w.N.
8 LAG Mecklenburg-Vorpommern, Urteil vom 12.11.2014, 3 TaBV 5/14
9 Kort, ZD 2016, 3, 5

**Öffentlich zugänglich** sind nicht nur solche Räume, die dem öffentlichen Verkehr gewidmet sind, sondern auch solche, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten oder benutzt werden können. Dabei ist der Begriff „Raum" weit auszulegen und im Sinne von „Bereich" zu verstehen.[1] Dazu gehören Kirchen, Eingangsbereiche von Krankenhäusern und Alten- sowie Pflegeheimen und sozialen Einrichtungen, Cafés, öffentlich zugängliche Außenanlagen. Aber auch Pfarrsäle, Jugendtreffs, Sozialstationen und das Pfarrbüro, soweit es den allgemein zugänglichen Teil betrifft, ebenso Eingangsbereiche und Treppenaufgänge zu Geschäftsräumen von Bürogebäuden.[2] 705

Auch **Schulhöfe** stellen öffentlich zugängliche Räume dar, solange der Schulbetrieb stattfindet. Außerhalb des Schulbetriebes, wenn das Schulgelände geschlossen ist, macht der Verantwortliche deutlich, dass er den Zugang zu diesen Räumen nicht mehr gestattet. 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.[3] Unerheblich ist, ob für den Zugang weitere Voraussetzungen, wie z. B. der Erwerb einer Eintrittskarte oder eine vorherige Anmeldung, erforderlich sind. 710

Die Videoüberwachung muss zur Wahrung des Hausrechts **oder** zur Wahrung berechtigter Interessen erforderlich sein: 715

Das Hausrecht stellt die Befugnis dar, darüber zu entscheiden, wer das Gebäude betreten und sich darin aufhalten darf[4]. Die Grenze für die Ausübung des Hausrechts stellt die Grundstücksgrenze dar. Eine Einbeziehung von öffentlichen oder privaten Grundstücken, die an das eigene Grundstück angrenzen, ist durch das Hausrecht nicht mehr gedeckt.[5]

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. Weiterhin muss eine konkrete Zweckbestimmung vorliegen, das heißt, das konkrete Ziel der Überwachung muss benannt sein. Allgemeine Erklärungen wie „Gefahr von Diebstählen oder Sachbeschädigungen" werden dem nicht gerecht.[6]

1 Gola/Heckmann, § 4 Rn. 23-26
2 OVG Lüneburg, Urteil vom 29.9.2014, 11 LC 114/13
3 Wedde in DKWW, § 6 b Rn. 20
4 Gola/Heckmann, § 4 Rn. 35 mit Hinweis auf Scholz in Simitis, § 6b Rn. 73
5 Scholz in Simitis, Anhang zu Art. 6 Rn. 70
6 So auch BfDI 23. Tätigkeitsbericht Pkt. 12.1. (dort zum Thema Beschäftigtendatenschutz)

720 Die Regelung des § 52 erfasst nur Videoüberwachungen in öffentlich zugänglichen Räumen. Im Umkehrschluss bedeutet dies, dass in nicht öffentlich zugänglichen Räumen § 52 KDG keine Anwendung findet. Soll eine **Videoüberwachung im Zusammenhang mit einem Beschäftigungsverhältnis** erfolgen, richtet sich die Zulässigkeit nach § 53 Abs. 2 KDG.

725 Voranzustellen ist, dass prägend für den Datenschutz im Beschäftigungsverhältnis das Verbot der „Totalüberwachung" des Mitarbeitenden ist.[1] Unabhängig davon, ob eine Videoüberwachung durch Aufzeichnung oder durch direkte Beobachtung an einem Überwachungsmonitor erfolgt, ist die freie Entfaltung der Persönlichkeit des Mitarbeitenden beeinträchtigt und erzeugt einen mit der Wahrung dieser Persönlichkeitsrechte nicht zu vereinbarenden Überwachungsdruck.[2] Das gilt gleichermaßen für die permanente, aber auch für punktuelle Aufzeichnungen. Wenn Mitarbeitenden zwar grundsätzlich bekannt ist, dass eine Videoüberwachung zeitweise erfolgt, sie aber nicht wissen, in welchem Moment die Kamera aufnimmt, ist damit ebenso ein permanenter Überwachungsdruck verbunden.[3]

730 Auch eine **offene Videoüberwachung** stellt einen nicht zulässigen Eingriff in das Persönlichkeitsrecht Mitarbeitender dar, wenn sich die Videoaufzeichnung nicht mit überwiegenden Interessen des Arbeitgebers oder mit konkreten Sicherheitsinteressen rechtfertigen lässt.[4] Besteht für eine Videoüberwachung grundsätzlich eine Rechtfertigung in diesem Sinne, dürfen die zu diesen Zwecken angebrachten Kameras nicht so eingestellt sein, dass damit eine Überwachung der Arbeitsplätze verbunden ist.[5]

735 Eine Überwachung von Mitarbeitern mit Hilfe einer **versteckten Kamera,** von der die Mitarbeitenden keine Kenntnis haben, ist grundsätzlich unzulässig, weil sie dem Transparenzgebot widerspricht.[6] Eine Ausnahme besteht dann, wenn konkrete, zu dokumentierende Anhaltspunkte einer strafbaren Handlung oder einer anderen schweren Verfehlung zulasten des Arbeitgebers bestehen, 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.[7] Eine bloß abstrakte Gefahr ist also nicht ausreichend.[8] In jedem Fall unzulässig sind Videoüberwachungen in Intimbereichen wie Toiletten, geschlossenen Sanitärbereichen (z. B. Duschen) und Umkleideka-

1 Kort, RdA 2018, 24
2 BAG, Beschluss vom 26. 8. 2008, 1 ABR 16/07 (Rn. 15)
3 Gola, Datenschutz am Arbeitsplatz, Rn. 78
4 Däubler, Rn. 312
5 Ebd, Rn. 312c
6 Maschmann in Kühling/Buchner, § 26 Rn. 21, 22
7 BAG, Urteil vom 20.10.2016, 2 AZR 395/15; BAG, Urteil vom 27.3.2003, 2 AZR 51/02; a.A. Maschmann, § 26 Rn. 22
8 Seifert in Simitis, Art. 88 Rn. 138; Däubler, Rn. 306

binen. Nicht zuletzt weil eine solche scheinbar selbstverständliche Regelung nicht in jedem Fall akzeptiert wurde, ist mit § 201a StGB eine Norm eingeführt worden, die unbefugte Bildaufnahme einer anderen Person, die sich in einem gegen Einblick besonders geschützten Raum befindet, unter Strafandrohung stellt.

## 7. Beschäftigtendatenschutz

740 In Artikel 88 DSGVO wird den Nationalstaaten das Recht eingeräumt, eigene Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext zu erlassen.

745 Der deutsche Gesetzgeber hat sich zunächst weitgehend damit begnügt, die Regelungen des § 32 BDSG a. F. in die Regelungen des § 26 BDSG n. F. zu übertragen. Obwohl der Bundestag bereits in der 17. Legislaturperiode einen Entwurf für einen Beschäftigtendatenschutz beschlossen hatte,[1] der dann an der Ablehnung im Bundesrat scheiterte, ist auch die Chance, ein solches Gesetz im Rahmen des Datenschutzanpassungsumsetzungsgesetzes mit zu beschließen, nicht umgesetzt worden. Neben der Übernahme der alten gesetzlichen Regelung sind aber einige Erweiterungen in den Abs. 2 ff. zu finden, die z. T. die bisher im Rahmen der Rechtsprechung entwickelten Regeln aufnehmen.

750 Die Vorschrift in § 53 KDG ist an die neue gesetzliche Terminologie angepasst, aber ansonsten wortgleich aus § 10 a KDO übernommen worden. Nach § 53 KDG dürfen *„personenbezogenen Daten eines Beschäftigten einschließlich der Daten über die Religionszugehörigkeit, der religiösen Überzeugung und die Erfüllung von Loyalitätsobliegenheiten für die Zwecke des Beschäftigungsverhältnisses verarbeitet werden …“,* wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

### 7.1 Beschäftigte

755 Wer die Beschäftigten sind, auf die die Vorschrift des § 53 KDG anzuwenden ist, regelt § 4 Nr. 24 KDG. Danach fallen grundsätzlich alle im Rahmen eines Beschäftigungs- oder Beamtenverhältnisses in einer Einrichtung tätigen Mitarbeitende darunter. Erfasst sind u. a. ausdrücklich auch Praktikanten, Auszubildende, Rehabilitanden, im Rahmen des Bundesfreiwilligendienstes tätige Personen und solche, die in Werkstätten für Menschen mit Behinderung tätig sind.

1 BT-Drucks. 17/4230

### 7.2 Daten der Religionszugehörigkeit

760 In Folge der Rechtsprechung des Europäischen Gerichtshofs darf die Religionszugehörigkeit aber als Voraussetzung für eine Einstellung nicht mehr für jede Stelle pauschal verlangt werden. Der EuGH verlangt dagegen einen objektiv überprüfbaren direkten Zusammenhang zwischen der Religionszugehörigkeit und der fraglichen Tätigkeit. Dieser kann sich aus der Art der Tätigkeit (z. B. Aufgaben der Verkündigung) oder aus den Umständen ihrer Ausübung ergeben. Dies wird insbesondere bei Leitungspositionen der Fall sein, in denen der Amtsinhaber die Position der Kirche glaubwürdig vertreten muss (etwa Leitung einer katholischen Kindertagestätte oder anderer kirchlicher Einrichtungen).[1]

765 Aufgrund dieser Rechtsprechung fehlt für die pauschale Frage nach der Religionszugehörigkeit im Kontext einer Bewerbungssituation der Zweck. Demgegenüber ist die Frage auf einem Personalbogen aber von einem Zweck getragen, wenn der Arbeitgeber verpflichtet ist, im Falle der Religionszugehörigkeit Kirchensteuern abzuführen.[2]

#### 7.2.1 Religiöse Überzeugung

770 In Bewerbungsgesprächen ist zu prüfen, ob in den Fällen, in denen die Religionszugehörigkeit nicht bereits aus der Stellenausschreibung eindeutig hervorging (Leitungsposition, pastorale und katechetische Stellen), die geforderte notwendige Identifikation mit den Aufgaben, Zielen und Werten der katholischen Kirche vorhanden ist.

775 Nicht erlaubt ist hingegen, den potentiellen Arbeitnehmer unmittelbar nach der Religionszugehörigkeit zu fragen oder aus der Nichtoffenlegung der Religionszugehörigkeit eine Benachteiligung des Bewerbers abzuleiten. Unschädlich ist jedoch, wenn der Bewerber von sich aus seiner Religionszugehörigkeit mitteilt.[3]

#### 7.2.2 Loyalität zur katholischen Kirche

780 Die Einhaltung der Grundordnung des kirchlichen Dienstes im Rahmen kirchlicher Arbeitsverhältnisse (GrO) ist regelmäßig Inhalt eines Arbeitsvertrages im kirchlichen Dienst. Die GrO formuliert in Artikel 4 bestimmte **Loyalitätsobliegenheiten,** nach denen von katholischen Mitarbeiterinnen und Mitarbeitern erwartet wird, dass sie die Grundsätze der katholischen Glaubens- und Sittenlehre anerkennen und beachten. Von nicht katholischen christlichen Mitarbeitenden wird erwartet, dass sie das Evangelium achten. Nichtchristliche Mitarbeitende müssen bereit sein, die ihnen in einer kirchlichen Einrichtung zu übertragenden Aufgaben im

1 Amtsblatt Bistum Magdeburg vom 1.7.2019, Nr. 78
2 Ebd.
3 Ebd.

Sinn der Kirche zu erfüllen. Alle Mitarbeitende haben kirchenfeindliches Verhalten zu unterlassen. Sie dürfen in ihrer persönlichen Lebensführung und in ihrem dienstlichen Verhalten die Glaubwürdigkeit der Kirche und der Einrichtung, in der sie beschäftigt sind, nicht gefährden.

Ausdrücklich erlaubt ist weiterhin die **Frage nach einem Kirchenausstritt.** 785
Wer aus der katholischen Kirche ausgetreten ist, hat sich klar von der Kirche abgewandt und kann nicht gleichzeitig widerspruchsfrei beteuern, sich mit den Werten und Zielen der katholischen Kirche zu identifizieren. Er verstößt damit gegen das Gebot der Mindestloyalität. Im Falle des Austritts aus der evangelischen Kirche ist die Identifikation mit den Zielen und Grundsätzen der katholischen Kirche mit den unten aufgeführten Fragen zu klären.

Um die Identifikation weiterhin zu prüfen, bieten sich verschiedene Fragen an:

- Was verbinden Sie mit christlichen Werten?
- Warum haben Sie sich bei einer katholischen Einrichtung beworben?
- Welche Erwartungen und Wünsche haben Sie an einen katholischen Arbeitgeber als Dienstgeber?
- Was verbindet Sie mit der katholischen Kirche / Caritas?[1]

## 7.3 Erforderlichkeit

Die Verarbeitung personenbezogener Daten muss geeignet und zugleich 790
das relativ mildeste Mittel sein, um die unternehmerischen Interessen und Zwecke bei der Durchführung des Beschäftigungsverhältnisses zu verwirklichen. Dementsprechend verpflichtet das Erforderlichkeitsprinzip stets zum Vergleich alternativer Handlungsformen und zwingt den Arbeitgeber zur Datenvermeidung und Datensparsamkeit, wo immer dies möglich ist. Der Beschäftigte muss seine Daten nur dann preisgeben, wenn der Arbeitgeber ohne ihre Kenntnis im konkreten Einzelfall eine legitime Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann.[2] Außerdem muss der Eingriff in die Persönlichkeitssphäre der betroffenen Person in einem angemessenen Verhältnis zu dem verfolgten Ziel stehen. Dies verpflichtet zu einer Abwägung der beiderseitigen Interessen.[3]

## 7.4 Einwilligung im Beschäftigungskontext

Ob eine Einwilligung im Zusammenhang mit einem Beschäftigungsver- 795
hältnis freiwillig abgegeben werden kann, war lange Zeit umstritten. So hatte der BGH entschieden, dass es an der Möglichkeit einer freien Entscheidung fehlen kann, wenn die Einwilligung in einer Situation wirt-

1 Amtsblatt Bistum Magdeburg vom 1.7.2019, Nr. 78
2 Ratgeber Beschäftigtendatenschutz, LbfDI Baden-Württemberg S. 8
3 Däubler, Rn. 183i

schaftlicher oder sozialer Schwäche oder Unterordnung erteilt wird.[1] Das BAG entschied hingegen, auch im Rahmen eines Arbeitsverhältnisses könnten sich Arbeitnehmer grundsätzlich „frei entscheiden", wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben wollten. Dem stünde weder die Tatsache abhängiger Beschäftigung noch das Weisungsrecht des Arbeitgebers entgegen. In der Literatur wurde die Ansicht vertreten, dass ein genereller Ausschluss der Einwilligung aufgrund des Über-Unterordnungsverhätnisses besteht,[2] dass man zwar nicht von einem generellen Ausschluss ausgehen darf, aber eine Vermutung gegen die Freiwilligkeit spricht,[3] bzw. der im Arbeitsverhältnis abgegebenen Einwilligung ein besonderes Augenmerk zu widmen ist.[4]

Im staatlichen Bereich ist diese Frage jetzt in § 26 BDSG geregelt, indem die Einwilligung im Zusammenhang mit dem Beschäftigungsverhältnis zumindest grundsätzlich statthaft ist. § 26 Abs. 2 BDSG fordert aber über diese Feststellung hinaus, für die Beurteilung der Freiwilligkeit einer Einwilligungserklärung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Eine dementsprechende Formulierung ist im KDG nicht aufgenommen, gleichwohl ist diese Abhängigkeitslage auch im kirchlichen Dienstverhältnis zu berücksichtigen. Dem steht die Tatsache, dass es sich in diesem Verhältnis um eine Dienstgemeinschaft handelt, nicht entgegen. Für die Antwort auf die Frage, ob eine Einwilligung im Rahmen eines kirchlichen Beschäftigungsverhältnisses freiwillig abgegeben werden kann, sind im Einzelfall die Kriterien des § 26 Abs. 2 BDSG heranzuziehen. Ebenso wie die von Thüsing vorgeschlagenen Kriterien, nach denen die Einwilligung zulässig ist, wenn:

- die Einwilligung erst erteilt wird, wenn sich die Parteien verbindlich auf die Begründung eines Beschäftigungsverhältnisses geeinigt haben,
- dem Beschäftigten ausreichend Zeit zur Entscheidung gegeben wird (mindestens drei Tage),
- der Beschäftigte die Möglichkeit hat, Rücksprache mit Dritten zu halten,
- der Beschäftigte auf diese Möglichkeit hingewiesen wurde.[5]

Insbesondere kann **Freiwilligkeit** angenommen werden, wenn die Datenverarbeitung für den Arbeitnehmer lediglich mit einem rechtlichen oder wirtschaftlichen Vorteil verbunden ist. Dies kann z. B. bei der Einführung

1 BGH, DB 2008, 2188 – diese Entscheidung betraf allerdings keinen arbeitsrechtlichen Fall
2 Simitis in Simitis, § 4a Rn. 62
3 Däubler, Art. 4 a BDSG a. F. Rn. 23
4 Ernst in Paal/Pauly, Art. 4 Rn. 71
5 Thüsing, NZA 2011, 18

eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen[1], der Aufnahme in konzernweite Personalentwicklungssysteme oder der Vergabe von Firmenrabatten[2] der Fall sein. Auch die Verfolgung **gleichgerichteter Interessen** spricht für die Freiwilligkeit einer Einwilligung. Hierzu kann nach der Begründung für das Datenschutzanpassungsumsetzungsgesetz etwa die Aufnahme von Namen und Geburtsdatum in eine Geburtstagsliste[3] oder die Nutzung von Fotos für das Intranet zählen, bei der Arbeitgeber und Beschäftigter im Sinne eines betrieblichen Miteinanders zusammenwirken.

1 BT-Drucks. 18/11325, S. 97.
2 Ernst in Paal/Pauly, Art. 4 Rn. 71
3 BT-Drucks. 18/11325, S. 97

# D 1 Datenschutz

## Beschäftigtendatenschutz