NomosKommentar

Sydow [Hrsg.]

# Kirchliches Datenschutzrecht

## Datenschutzbestimmungen der katholischen Kirche

Handkommentar

Nomos

Lambertus

NomosKommentar

**Prof. Dr. Gernot Sydow, M.A.** [Hrsg.]

# Kirchliches Datenschutzrecht

## Datenschutzbestimmungen der katholischen Kirche

### Handkommentar

**Marcus Baumann-Gretza**, Justitiar des Erzbistums Paderborn, Leiter der Unterkommission Datenschutz- und Melderecht/IT-Recht der VDD-Rechtskommission | **Ursula Becker-Rathmair**, Diözesandatenschutzbeauftragte, Leiterin des Katholischen Datenschutzzentrums Frankfurt/Main | **Andreas Braun**, M.A., LL.M., Universität Münster | **Raimund J. Evers**, Juristischer Referent, Katholisches Datenschutzzentrum, Dortmund | **Dr. Martin Fuhrmann**, Leiter der Rechtsabteilung beim Verband der Diözesen Deutschlands | **Dr. Danielle Gaukel**, Syndikusrechtsanwältin, Bischöfliches Ordinariat Limburg | **Prof. Dr. Felix Hammer**, Diözesanjustitiar und Kanzler, Bistum Rottenburg-Stuttgart | **Prof. Dr. Ansgar Hense**, Direktor des Instituts für Staatskirchenrecht der Diözesen Deutschlands, Bonn | **Maike Herrlein**, Universität Münster/Erzbischöfliches Generalvikariat Paderborn, Abteilung Weltliches Recht | **Stephanie Melzow**, Juristische Referentin, Katholisches Datenschutzzentrum, Dortmund | **Steffen Pau**, Diözesandatenschutzbeauftragter, Leiter des Katholischen Datenschutzzentrums, Dortmund | **Prof. Dr. Peter Platen**, Leiter der Abteilung Kirchliches Recht und Kanzler der Kurie, Bischöfliches Ordinariat Limburg; apl. Professor für Kirchenrecht, Universität Münster | **Alexandra Recke**, Juristische Referentin, DOK Deutsche Ordensobernkonferenz e.V. | **Prof. Dr. Martin Rehak,** Professor für Kirchenrecht, Universität Würzburg, Richter am Interdiözesanen Datenschutzgericht | **Prof. Dr. Ulrich Rhode SJ**, Ordentlicher Professor für Kirchenrecht, Pontificia Università Gregoriana, Rom | **Dr. Markus Schulten**, Juristischer Referent am Institut für Staatskirchenrecht der Diözesen Deutschlands, Bonn | **Pia Marie Siebert**, Universität Münster | **Prof. Dr. Gernot Sydow**, M.A., Universität Münster, Vorsitzender des Datenschutzgerichts der Deutschen Bischofskonferenz | **Matthias Ullrich**, Datenschutzbeauftragter der ostdeutschen Bistümer und des Katholischen Militärbischofs, Schönebeck | **Johanna Werpers**, Universität Münster

Nomos

Lambertus

**Zitiervorschlag:** HK-Kirchliches DatenschutzR

**Die Deutsche Nationalbibliothek** verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8487-6255-2 (Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden)

ISBN 978-3-7841-3308-9 (Lambertus-Verlag GmbH, Freiburg)

1. Auflage 2021

## Vorwort

Das Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 hat einen grundlegenden Umbruch im Datenschutzrecht bedeutet. Die katholische Kirche hat zum selben Zeitpunkt ihr in den deutschen Diözesen geltendes Datenschutzrecht durch das Kirchliche Datenschutzgesetz (KDG) und weitere Datenschutzbestimmungen mit der DS-GVO in Einklang gebracht.

Die Anwendung des kirchlichen Datenschutzrechts kann sich vielfach an den Parallelbestimmungen der DS-GVO und des BDSG orientieren. Anwendungsschwierigkeiten ergeben sich, soweit das kirchliche Datenschutzrecht im Einzelfall abweichende Regelungen enthält. An diesem Punkt setzt der vorliegende Kommentar an: Er konzentriert sich auf die Spezifika des kirchlichen Datenschutzrechts und verzichtet auf umfassende Kommentierungen, soweit das kirchliche Recht der DS-GVO bzw. dem BDSG entspricht. Dieser Kommentar zum Datenschutzrecht der katholischen Kirche ergänzt damit die in derselben Reihe erschienenen Kommentierungen der DS-GVO (Sydow, Hrsg., Europäische Datenschutzgrundverordnung, 2. Aufl. 2018) und des BDSG (Sydow, Hrsg., Bundesdatenschutzgesetz, 1. Aufl. 2020).

Leges authentice interpretatur legislator (can. 16 § 1 CIC). Der vorliegende Kommentar stützt sich daher nicht auf Amtsautorität, sondern auf die Überzeugungskraft der Positionen, die die Autorinnen und Autoren vertreten. Sie sind in verantwortlichen Positionen in den kirchlichen Verwaltungen und Datenschutzaufsichten, beim Verband der Diözesen Deutschlands, in der kirchlichen Gerichtsbarkeit oder in der Wissenschaft mit Fragen des kirchlichen Datenschutzes befasst. Die Aufgaben des Herausgebers sind durch die Mitarbeiterinnen und Mitarbeiter des Instituts für internationales und vergleichendes öffentliches Recht der Universität Münster in vielfältiger Weise unterstützt worden. Den Autorinnen und Autoren, meinen Mitarbeiterinnen und Mitarbeitern und nicht zuletzt dem Nomos-Verlag danke ich für die hervorragende Zusammenarbeit während der Entstehung dieses Kommentars.

Münster, im Oktober 2020 Gernot Sydow

## Bearbeiterverzeichnis

*Marcus Baumann-Gretza,*
Justitiar des Erzbistums Paderborn, Leiter der Unterkommission Datenschutz- und Melderecht/IT-Recht der VDD-Rechtskommission

*Ursula Becker-Rathmair*,
Diözesandatenschutzbeauftragte, Leiterin des Katholischen Datenschutzzentrums Frankfurt/Main

*Andreas Braun, M.A., LL.M.*,
Universität Münster

*Raimund J. Evers*,
Juristischer Referent, Katholisches Datenschutzzentrum, Dortmund

*Dr. Martin Fuhrmann*,
Leiter der Rechtsabteilung beim Verband der Diözesen Deutschlands

*Dr. Danielle Gaukel*,
Syndikusrechtsanwältin, Bischöfliches Ordinariat Limburg

*Prof. Dr. Felix Hammer*,
Diözesanjustitiar und Kanzler, Bistum Rottenburg-Stuttgart

*Prof. Dr. Ansgar Hense*,
Direktor des Instituts für Staatskirchenrecht der Diözesen Deutschlands, Bonn

*Maike Herrlein*,
Universität Münster/Erzbischöfliches Generalvikariat Paderborn, Abteilung Weltliches Recht

*Stephanie Melzow*,
Juristische Referentin, Katholisches Datenschutzzentrum, Dortmund

*Steffen Pau*,
Diözesandatenschutzbeauftragter, Leiter des Katholischen Datenschutzzentrums, Dortmund

*Prof. Dr. Peter Platen*,
Leiter der Abteilung Kirchliches Recht und Kanzler der Kurie, Bischöfliches Ordinariat Limburg; apl. Professor für Kirchenrecht, Universität Münster

*Alexandra Recke*,
Juristische Referentin, DOK Deutsche Ordensobernkonferenz e.V.

*Prof. Dr. Martin Rehak*,
Professor für Kirchenrecht, Universität Würzburg, Richter am Interdiözesanen Datenschutzgericht

*Prof. Dr. Ulrich Rhode SJ*,
Ordentlicher Professor für Kirchenrecht, Pontificia Università Gregoriana, Rom

*Dr. Markus Schulten*,
Juristischer Referent am Institut für Staatskirchenrecht der Diözesen Deutschlands, Bonn

*Pia Marie Siebert*,
Universität Münster

*Prof. Dr. Gernot Sydow, M.A.*,
Universität Münster, Vorsitzender des Datenschutzgerichts der Deutschen Bischofskonferenz

*Matthias Ullrich*,
Datenschutzbeauftragter der ostdeutschen Bistümer und des Katholischen Militärbischofs, Schönebeck

*Johanna Werpers*,
Universität Münster

Im Einzelnen haben bearbeitet:

| | |
|---|---|
| Marcus Baumann-Gretza | § 14 KDG-DVO |
| Ursula Becker-Rathmair | § 51 KDG |
| Andreas Braun, M.A., LL.M. | §§ 39–41, 56–58 KDG, 18–20 KDG-DVO |
| Raimund J. Evers | §§ 42, 43 KDG |
| Dr. Martin Fuhrmann | §§ 52, 53 KDG |
| Dr. Danielle Gaukel | §§ 8, 17 KDG |
| Prof. Dr. Felix Hammer | §§ 2, 3 KDG |
| Prof. Dr. Ansgar Hense | §§ 44–46, 54 KDG |
| Maike Herrlein | §§ 4, 26, 48–50 KDG, 6, 7, 9–13 KDG-DVO |
| Stephanie Melzow | § 47 KDG |
| Steffen Pau | §§ 33, 34, 42, 43, 47 KDG, 2–5, 8, 15–17, 21–26 KDG-DVO |
| Prof. Dr. Peter Platen | § 18 KDG |
| Alexandra Recke | Einführung zur KDR-OG |
| Prof. Dr. Martin Rehak | §§ 9, 10 KDG |
| Prof. Dr. Ulrich Rhode SJ | Präambel zum KDG, Einführung zur KDSGO |
| Dr. Markus Schulten | §§ 36–38 KDG |
| Pia Marie Siebert | §§ 5, 6, 7, 13, 14, 19–24, 27, 28, 32, 35 KDG, 27, 28 KDG-DVO |
| Prof. Dr. Gernot Sydow, M.A. | Einführung zum KDG, §§ 1, 5, 7, 13, 14, 19–24, 27, 28, 32, 35 KDG, 27, 28 KDG-DVO |
| Matthias Ullrich | §§ 11, 12, 15, 16, 25, 55 KDG |
| Johanna Werpers | §§ 6, 29–31 KDG, 1 KDG-DVO |

## Inhaltsverzeichnis

**Kapitel 5**
**Übermittlung personenbezogener Daten an und in Drittländer oder an internationale Organisationen**



**Kapitel 6**
**Datenschutzaufsicht**



**Kapitel 7**
**Beschwerde, gerichtlicher Rechtsbehelf, Haftung und Sanktionen**



**Kapitel 8**
**Vorschriften für besondere Verarbeitungssituationen**



**Kapitel 9**
**Übergangs- und Schlussbestimmungen**

**Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)**

**Kapitel 1**
**Verarbeitungstätigkeiten**



**Kapitel 2**
**Datengeheimnis**



**Kapitel 3**
**Technische und organisatorische Maßnahmen**

**Abschnitt 1: Grundsätze und Maßnahmen**



**Abschnitt 2: Schutzbedarf und Risikoanalyse**



**Kapitel 4**
**Maßnahmen des Verantwortlichen und des Mitarbeiters**



**Kapitel 5**
**Besondere Gefahrenlagen**

**Kapitel 6**
**Übergangs- und Schlussbestimmungen**



**Kirchliche Datenschutzgerichtsordnung (KDSGO)**

**Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG)**

# Gesetz über den Kirchlichen Datenschutz (KDG)

## Einführung



### I. Die DS-GVO als europarechtlicher Rechtsrahmen des kirchlichen Datenschutzrechts

Die europäische **Datenschutz-Grundverordnung** (**DS-GVO**)[1] hat das Datenschutzrecht mit ihrem Inkrafttreten am 25. Mai 2018 grundlegend umgestaltet, und zwar auf zahlreichen Ebenen: im materiellen Datenschutzrecht ebenso wie auf institutioneller und verfahrensrechtlicher Ebene mit Neuregelungen zum Datenschutzbeauftragten, zu den Aufsichtsbehörden, zu Rechtsbehelfen, Haftung und Sanktionen.[2] Die DS-GVO normiert demzufolge nicht allein das materielle Datenschutzrecht, sondern regelt auch – in einem weit verstandenen Sinn – seine **Durchsetzung**. 1

Das Inkrafttreten der europäischen Datenschutz-Grundverordnung hat auch das **kirchliche Datenschutzrecht** nicht unberührt gelassen. Zwar billigt Art. 91 Abs. 1 DS-GVO den Kirchen weiterhin den Freiraum zu, kircheneigenes anstelle des staatlichen Datenschutzrechts anzuwenden. Sie stellt dies aber unter die Bedingung, dass die kirchlichen Regelungen mit der DS-GVO in Einklang stehen (näher unten → Rn. 18 ff.). 2

Die DS-GVO beruht auf dem Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf **Art. 16 AEUV**.[3] Dessen Absatz 1 normiert in Entsprechung zu Art. 8 GRCh das Recht auf Schutz personenbezogener Daten. Art. 8 Abs. 1 GRCh und Art. 16 Abs. 1 AEUV gewährleisten beide den Schutz personenbezogener Daten. Dieses **Datenschutzgrundrecht** bildet den 3

1 VO (EU) Nr. 2016/697 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG, ABl. 2016 Nr. L 119/1; Geltung seit 25.5.2018.
2 Art. 37 ff., 77 ff. DS-GVO.
3 Einleitungssatz zur DS-GVO vor den Erwägungsgründen.

normativen Rahmen, in dem das datenschutzrechtliche Sekundärrecht der Union zu entwickeln ist, und ist daher für Verständnis und Auslegung dieses Sekundärrechts von grundlegender Bedeutung.[4]

4 Art. 16 Abs. 2 AEUV überträgt der Europäischen Union die **Kompetenz**, im ordentlichen Gesetzgebungsverfahren[5] Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und über den freien Datenverkehr zu treffen. Voraussetzung ist indes, dass es sich um Tätigkeiten handelt, die in den Anwendungsbereich des Unionsrechts fallen (→ Rn. 7 ff.).

5 Die Kompetenztitel des Europarechts dienen vielfach nicht nur der Begründung einer Verbandskompetenz der EU und der Bestimmung von Organkompetenzen und Handlungsformen für die Sekundärrechtsetzung, sondern auch der Normierung einzelner inhaltlicher Vorgaben für das Sekundärrecht. So bestimmt Art. 16 Abs. 2 S. 2 AEUV bereits auf primärrechtlicher Ebene, dass die Einhaltung der Datenschutzbestimmungen von **unabhängigen Behörden** überwacht werden müsse. Die DS-GVO setzt diese Vorgabe, die bereits vor Erlass der DS-GVO durch die Rechtsprechung des EuGH[6] nähere Konturen gewonnen hatte, durch Art. 52 DS-GVO um. Die Norm enthält Bestimmungen zur Unabhängigkeit und Weisungsfreiheit der Mitglieder der Aufsichtsbehörde, Inkompatibilitätsregelungen und Bestimmungen über die personellen, technischen und finanziellen Ressourcen der nationalen Aufsichtsbehörden, die auch für die kirchlichen Datenschutzaufsichten relevant sind.

6 Durch die DS-GVO ist ein **normatives Mehrebenensystem** entstanden.[7] Neben dem europäischen Primärrecht und der DS-GVO ist vor allem wegen der ausfüllungsbedürftigen Öffnungsklauseln der DS-GVO auch nationales Datenschutzrecht unmittelbar anwendbar, in Deutschland wie bisher teils auf Bundes-, teils auf Landesebene. Das BDSG und die Landesdatenschutzgesetze mussten dementsprechend neugefasst werden. Im Ergebnis erschwert das Nebeneinander von europäischem und nationalem Datenschutzrecht die Rechtsanwendung. Für den kirchlichen Bereich treten inhaltliche Abweichungen des kirchlichen Datenschutzrechts hinzu, das zwar nicht in seinem generellen Schutzstandard, wohl aber in zahlreichen Einzelpunkten eigenständige Regelungen enthält.

## II. Begrenzte Anwendbarkeit der DS-GVO auf das Handeln der Kirchen aus Kompetenzgründen

### 1. Prinzip der begrenzten Einzelermächtigung

7 Im Zentrum der Diskussion über kirchliche Regelungsfreiräume im Datenschutzbereich steht üblicherweise Art. 91 DS-GVO, der eine Öffnungsklausel zugunsten kirchlicher Regelungen enthält (→ Rn. 2). Diese Öffnungsklausel

4 Vgl. EuGH 20.5.2003 – C-465/00, ECLI:EU:C:2003:294 Rn. 68 – Österreichischer Rundfunk ua.

5 Dh durch übereinstimmende Mehrheitsentscheidungen im Europäischen Parlament und im Rat; im Einzelnen: Art. 294 AEUV.

6 EuGH 9.3.2010 – C-518/07, ECLI:EU:C:2010:125 – Kommission/Deutschland; EuGH 16.10.2012 – C-614/10, ECLI:EU:C:2012:631 – Kommission/Österreich; EuGH 8.4.2014 – C-293/12 und C-594/12, ECLI:EU:C:2014:238 – Digital Rights Ireland und Seitlinger ua; dazu auch von der Groeben/Schwarze/Hatje/Brühann AEUV Art. 16 Rn. 76 ff.; von Lewinski ZG 2015, 228 ff.

7 So Benecke/Wagner DVBl. 2016, 600 (600).

kann aber nur und erst dann von Bedeutung sein, wenn der **Anwendungsbereich des Unionsrechts** grundsätzlich eröffnet ist. Nur soweit die EU grundsätzlich überhaupt eine Kompetenz hat, die Tätigkeiten der Kirchen dem europäischen Datenschutzrecht zu unterwerfen, kann es auf eine Öffnungsklausel und den darin liegenden Verzicht auf die Setzung unmittelbar anwendbaren Unionsrechts in diesem Bereich ankommen. Die Kompetenzfrage liegt somit der Frage nach Umfang und Interpretation des Art. 91 DS-GVO voraus.

Gemäß Art. 16 Abs. 2 AEUV besteht die Gesetzgebungskompetenz der EU für die Verarbeitung personenbezogener Daten für zwei Konstellationen: Datenverarbeitungen durch die Organe, Einrichtung und sonstigen Stellen der EU sowie Datenverarbeitungen durch die Mitgliedstaaten, im zweiten Fall nur im Rahmen von Tätigkeiten im Anwendungsbereich des Unionsrechts. Dementsprechend ist die DS-GVO gemäß Art. 2 Abs. 2 lit. a DS-GVO nur auf die Ausübung von Tätigkeiten anzuwenden, die in den **Anwendungsbereich des Unionsrechts** fallen. Diese Regelung ist Konsequenz des **Prinzips der begrenzten Einzelermächtigung**, nach dem Unionskompetenzen stets eine explizite kompetenzbegründende Norm in den Unionsverträgen voraussetzen. 8

Für Tätigkeiten außerhalb des grundsätzlichen Anwendungsbereichs des Unionsrechts fehlt es der EU an der Kompetenz, die für solche Tätigkeiten zu beachtenden Datenschutzregelungen aufzustellen. Dementsprechend normiert Teil 4 des BDSG ohne inhaltliche europarechtliche Vorgaben besondere Bestimmungen für Datenverarbeitungen im Rahmen von Tätigkeiten, die nicht in die Anwendungsbereiche der DS-GVO und der Richtlinie (EU) 2016/680 fallen. 9

### 2. Anwendungsbereich des Unionsrechts

Dass Teil 4 des BDSG nur wenige Bestimmungen enthält,[8] ist ein Hinweis darauf, dass der **Anwendungsbereich** des Unionsrechts **weit** zu fassen ist. Hierunter ist nicht nur die Datenverarbeitung durch Organe der EU und der Mitgliedstaaten bei der Durchführung von Unionsrecht zu verstehen. 10

Für einen darüber hinausgehenden Anwendungsbereich spricht der Vergleich zur Kompetenzgrundlage Art. 16 Abs. 2 AEUV. Denn anders als Art. 51 Abs. 1 GRCh, der den Anwendungsbereich der Unionsgrundrechte definiert, bezieht sich Art. 16 Abs. 2 AEUV gerade nicht nur auf die Durchführung des Unionsrechts im Sinne des gesetzgeberischen und administrativen Vollzugs europäischer Verordnungen und Richtlinien. Durch Art. 16 Abs. 2 AEUV sollte vielmehr ein **einheitlicher Kompetenztitel für das Datenschutzrecht** geschaffen werden, der die früher für den Datenschutz einschlägige Binnenmarktkompetenz aus dem damaligen Art. 95 EGV (heute Art. 114 AEUV) nicht einschränkt und daher auch die früheren europarechtlichen Daten- 11

8 §§ 85, 86 BDSG.

schutzregelungen wie die RL 95/46/EG umfasst.[9] Der Binnenmarktkompetenz unterfielen nach der Judikatur des EuGH auch rein innerstaatliche Datenverarbeitungen durch öffentliche und nichtöffentliche Stellen.[10] Entsprechendes gilt für Art. 16 Abs. 2 AEUV[11] und mithin für den Anwendungsbereich der DS-GVO.

12 Für Datenverarbeitungen durch Kirchen und Religionsgemeinschaften bedeutet dies: Insbesondere soweit ein Binnenmarktbezug einer Tätigkeit besteht oder jedenfalls entstehen könnte, ist der Anwendungsbereich des Unionsrechts eröffnet und wäre daher die DS-GVO anwendbar, wenn sie nicht die Bereichsausnahme zugunsten des kirchlichen Rechts in Art. 91 DS-GVO enthielte. Das betrifft beispielsweise die Erbringung von Gesundheitsdienstleistungen **in kirchlichen Krankenhäusern**, für die die Dienstleistungsfreiheit gilt und somit der Anwendungsbereich des Unionsrechts eröffnet ist.

13 Für nicht wenige kirchliche Datenverarbeitungen ist indes nicht ersichtlich, woraus sich ein Bezug zum Anwendungsbereich des Unionsrechts und damit die grundsätzliche Normierungskompetenz der EU ergeben sollten. Die Führung der **Kirchenbücher** (**Taufbuch etc**) verzeichnet kirchliche Amtshandlungen und hat somit zweifellos zwar einen Bezug zu personenbezogenen Daten, nicht aber einen Bezug zum Unionsrecht, was grundlegende Voraussetzung einer EU-Kompetenz für entsprechende Datenschutzregelungen wäre.

14 Sofern man das Prinzip der begrenzten Einzelermächtigung und den einschränkenden Wortlaut des Art. 16 Abs. 2 S. 1 AEUV nicht ignorieren will, verbleibt daher nur die Konsequenz, dass die DS-GVO bereits nach Art. 16 Abs. 2 S. 1 AEUV, Art. 2 Abs. 2 lit. a DS-GVO und nicht erst auf der Grundlage der Bereichsausnahme in Art. 91 DS-GVO auf einen beträchtlichen Teil des kirchlichen Handelns nicht anwendbar ist: nämlich für alle kirchlichen Handlungen außerhalb des zwar weit zu verstehenden, aber **nicht grenzenlosen Anwendungsbereichs** des Unionsrechts.

### 3. Konsequenzen für den kirchlichen Gesetzgeber

15 Der Unterschied zwischen einer **Nichtanwendbarkeit der DS-GVO** aufgrund von Art. 2 Abs. 2 DS-GVO oder aufgrund von Art. 91 DS-GVO ist deshalb relevant, weil die Bereichsausnahme des Art. 91 DS-GVO konditioniert ist. Die in Art. 91 DS-GVO statuierten Anforderungen an das kirchliche Datenschutzrecht – „in Einklang [mit der DS-GVO] gebracht werden" – greifen aber nur, soweit der Anwendungsbereich des Unionsrechts eröffnet ist. Außerhalb dieses Anwendungsbereichs war der kirchliche Gesetzgeber nicht ge-

9 von der Groeben/Schwarze/Hatje/Brühann AEUV Art. 16 Rn. 66; somit ist der Begriff des Anwendungsbereichs des Unionsrechts entsprechend dem des Art. 3 Abs. 2 RL 95/46/EG zu verstehen. Art. 16 Abs. 2 AEUV übernimmt jedoch nicht die zusätzlichen Einschränkungen des Art. 3 Abs. 2 RL 95/46/EG (öffentliche Sicherheit, Landesverteidigung, die Sicherheit des Staates, Tätigkeit des Staates im strafrechtlichen Bereich).

10 Zur Anwendung der RL 95/46/EG bei Verarbeitungen ohne Bezug zu den durch den EG-Vertrag garantierten Grundfreiheiten EuGH 20.5.2003 – C-465/00 und C-138/01 und C-139/01, ECLI:EU:C:2003:294 Rn. 41 ff. – Österreichischer Rundfunk ua; zur Anwendbarkeit der RL 95/46/EG auf Verarbeitungen durch Private EuGH 6.11.2003 – C-101/01, ECLI:EU:C:2003:596 Rn. 37 ff. – Lindqvist; zusammenfassend von der Groeben/Schwarze/Hatje/Brühann AEUV Art. 16 Rn. 67 ff.

11 So auch Sobotta in Grabitz/Hilf/Nettesheim AEUV Art. 16 Rn. 32.

halten, das kirchliche Datenschutzrecht in Einklang mit der DS-GVO zu bringen. Hierfür wären auch gänzlich von der DS-GVO abweichende Regelungen denkbar.

16 Die kirchlichen Gesetzgeber der evangelischen und katholischen Kirche in Deutschland haben diese **Differenzierungsoption** nicht genutzt, sei es weil sie im kirchlichen Gesetzgebungsverfahren überhaupt nicht im Blick war, sei es weil es gute Sachgründe gibt, auf eine Zweispurigkeit des kirchlichen Datenschutzrechts innerhalb und außerhalb des Anwendungsbereichs des Unionsrechts zu verzichten. Denn die einheitliche Regelung durch das KDG erspart die in Zweifelsfällen nicht einfache Abgrenzung, welches kirchliche Handeln in den Anwendungsbereich des Unionsrechts fällt und welches nicht. Zudem erleichtert ein einheitlich für das gesamte kirchliche Handeln geltendes KDG die praktische Rechtsanwendung innerhalb der Kirchen. Schließlich wird die kirchliche Autonomie durch die Umsetzung der Anforderungen des Art. 91 DS-GVO auch nicht ungebührlich beschränkt.

17 Angesichts der Existenz von Art. 91 DS-GVO und der Entscheidung des kirchlichen Gesetzgebers zur Normierung eines einheitlich für das gesamte kirchliche Handeln geltenden KDG (und paralleler Entscheidungen im Bereich der evangelischen Kirche) ist die Frage nach der Reichweite der unionsrechtlichen Kompetenzen für kirchliches Handeln damit **ohne aktuelle Relevanz**. Die Frage würde ihre Relevanz indes sofort zurückgewinnen, wenn Art. 91 DS-GVO gestrichen würde oder eine dezidiert restriktive Interpretation erfahren sollte. In einer solchen Situation wäre es von unmittelbarer Bedeutung, dass die EU wegen des Prinzips der begrenzten Einzelermächtigung das kirchliche Handeln für Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, aus Gründen fehlender Verbandskompetenzen nicht regeln kann und die DS-GVO insoweit ohnehin nicht anwendbar ist.

## III. Bereichsausnahme zugunsten kircheneigener Datenschutzbestimmungen nach Art. 91 DS-GVO

### 1. Zielsetzung des Art. 91 DS-GVO

18 Die Bereichsausnahme des Art. 91 DS-GVO zugunsten eigener Datenschutzbestimmungen der Kirchen und Religionsgemeinschaften verfolgt ein **doppeltes Ziel**: Einerseits soll das Recht des Einzelnen auf den Schutz seiner personenbezogenen Daten gewährleistet, andererseits der Status der Religionsgesellschaften geschützt werden, ihre Angelegenheiten selbst zu regeln und zu verwalten. Denn nach Art. 17 Abs. 1 AEUV achtet die Union den besonderen Status der Religionsgemeinschaften in den Mitgliedstaaten[12] und gewährleistet zugleich nach Art. 16 AEUV den Schutz personenbezogener Daten.

19 Dieses Doppelziel erreicht Art. 91 DS-GVO durch **eine gestufte, konditionierte Öffnungsklausel**.[13] Die DS-GVO ermöglicht die Anwendung von Datenschutzbestimmungen von **Kirchen und religiösen Vereinigungen** an Stelle der DS-GVO, sofern diese Bestimmungen mit der DS-GVO in Einklang gebracht

12 Vgl. hierzu nur Vedder in HK-UnionsR AEUV Art. 17 Rn. 6–9; Ziegenhorn/Drossel KuR 2016, 230 (231).

13 Die nachfolgende Darstellung des Regelungsgehalts von Art. 91 DS-GVO folgt weitgehend der Kommentierung dieser Bestimmung durch Hense in HK-DS-GVO, Art. 91 Rn. 1 ff.; für nähere Einzelheiten und Nachweise sei im Einzelnen auf diese Kommentierung verwiesen.

werden.[14] Unter dieser Voraussetzung ist die DS-GVO nicht anwendbar, sondern entfaltet gegenüber nicht-staatlichem, kirchlichem Recht eine richtlinienartige Wirkung. Art. 91 Abs. 1 DS-GVO räumt im kirchlichen Bereich den kircheneigenen Datenschutzregelungen Anwendungsvorrang[15] gegenüber den ansonsten unmittelbar verbindlichen Vorschriften der DS-GVO ein. Wie dargelegt (→ Rn. 15 ff.), setzt dies nach dem Prinzip der begrenzten Einzelermächtigung das Bestehen einer EU-Kompetenz voraus.

### 2. Anforderungen an die kirchliche Datenschutzgesetzgebung

20 Der Rechtsbegriff der „**umfassenden Regeln**" in Art. 91 DS-GVO ist dahin gehend zu verstehen, dass eine kohärente kirchliche Gesamtregelung des Datenschutzrechts vorliegen muss, die insbesondere nicht weiterführend durch staatliche Regelungen ergänzt werden muss.[16] Es liegt nahe, dass religions- und kircheneigene Regeln gleichsam als Regelungswerke mit kodifikatorischem Charakter konzipiert werden, die einen möglichst sämtliche relevanten Aspekte abdeckenden, systematischen Gesamtzusammenhang normieren.[17] Das Kriterium der umfassenden Regeln darf keinen überspannten Vollständigkeitsansprüchen ausgesetzt werden, da dies funktionale, religionsverfassungsrechtliche Regelungsspielräume unterminieren würde.[18]

21 **In Einklang bringen** muss etwas anderes bedeuten als völliges Übereinstimmen im Sinne von Deckungsgleichheit oder Identität.[19] Vielmehr muss es einen Gestaltungsspielraum des kirchlichen Rechtsetzers geben,[20] was sich gesetzessystematisch auch aus dem Vergleich zur strikteren Vorgabe des Art. 91 Abs. 2 DS-GVO schließen lässt.[21] Das gesetzgeberische Ermessen des religionsgesellschaftlichen Rechtsetzers ist dabei aber nicht völlig ungebunden oder schrankenlos. Der Korridor möglicher kircheneigener Normsetzung wird durch die strukturellen Leitideen und Grundsätze der DS-GVO „vorgespurt".[22]

### 3. Art. 91 DS-GVO als Bereichsausnahme

22 Nach teilweise vertretener Auffassung soll es sich bei Art. 91 Abs. 1 DS-GVO lediglich um eine **Bestandschutzregelung** handeln.[23] Diese Auffassung hat prima facie einen Teil des Wortlauts der Norm für sich, da Art. 91 Abs. 1 DS-GVO auf bestehende Datenschutzregelungen bezogen ist, die bereits im Zeitpunkt des Inkrafttretens der DS-GVO angewandt wurden. Andererseits sieht

14 Art. 91 Abs. 1 DS-GVO; Erwägungsgrund 165 DS-GVO; hierzu Hoeren NVwZ 2018, 373 (373 f.).
15 Ehmann/Kranig in Ehmann/Selmayr DS-GVO Art. 91 Rn. 10.
16 Herbst in Kühling/Buchner DS-GVO Art. 91 Rn. 10.
17 Hense in HK-DS-GVO Art. 91 Rn. 18.
18 Hense in HK-DS-GVO Art. 91 Rn. 18; Gola in ders. DS-GVO Art. 91 Rn. 16: es müsse sich nicht zwingend um „eine in sich geschlossene abschließende Regelung" handeln.
19 Hense in HK-DS-GVO Art. 91 Rn. 20.
20 Vgl. Herbst in Kühling/Buchner DS-GVO Art. 91 Rn. 14 f.; Pauly in Paal/Pauly DS-GVO Art. 91 Rn. 25. Ferner Jacob in Eßer/Kramer/v. Lewinski DS-GVO Art. 91 Rn. 13.
21 Ziegenhorn/Drossel Kirche und Recht 2016, 230 (241).
22 Hense in HK-DS-GVO, Art. 91 Rn. 21.
23 Herbst in Kühling/Buchner DS-GVO Art. 91 Rn. 13; Gola in Gola DS-GVO Art. 91 Rn. 1, 17.

Art. 91 Abs. 1 DS-GVO selbst eine Anpassung dieser Regelungen an die DS-GVO vor, erzwingt also deren Fortentwicklung und kann daher kein reiner Bestandsschutz zugunsten von Normbeständen sein, die im Zeitpunkt des Inkrafttretens der DS-GVO galten.

23 Auch die systematische Stellung des Art. 91 DS-GVO spricht gegen die Annahme einer Bestandsschutzregelung; stattdessen handelt es sich um eine **bereichsspezifische Regelung**. Denn Art. 91 DS-GVO steht nicht etwa in Kapitel XI der DS-GVO mit ihren Schlussbestimmungen und damit nicht in einem Kontext, in dem eine Bestandsschutzregelung zu erwarten wäre. Art. 91 DS-GVO ist vielmehr in Kapitel IX der DS-GVO platziert, das „Vorschriften für besondere Verarbeitungssituationen" enthält. Auch die übrigen Normen dieses Kapitels – beispielsweise für den Bereich der Medien, den Beschäftigungskontext oder Archive – sind stets durch sachliche Sonderregelungen, nicht aber durch temporale Beschränkungen ihres Anwendungsbereichs gekennzeichnet.

24 Jedenfalls soweit Kirchen und Religionsgemeinschaften beim Inkrafttreten der DS-GVO über umfassende Datenschutzbestimmungen verfügten, gewährleistet Art. 91 DS-GVO demzufolge nicht nur deren Bestand, sondern auch deren **Fortentwicklung**. So hat auch die damalige Bundesdatenschutzbeauftragte klargestellt, dass Änderungen des bestehenden religionseigenen Rechts möglich sind und sogar notwendig wurden.[24] Eine **Versteinerung** von Regeln, die zum Zeitpunkt des Erlasses der DS-GVO bestanden, kann **nicht Zweck** des Art. 91 DS-GVO sein.[25]

25 Diskutabel erscheint allein, ob sich der **institutionelle Anwendungsbereich** des Art. 91 DS-GVO auf solche Religionsgemeinschaften beschränken soll, die bereits am 24. Mai 2016 umfassende eigene Datenschutzregelungen hatten oder sie jedenfalls in den zwei Jahren des Übergangszeitraums bis zum Inkrafttreten der DS-GVO geschaffen haben. Die Frage ist für die katholische wie für die evangelische Kirche in Deutschland ohne Relevanz, weil mit der KDO entsprechende kirchliche Regelungen schon vor Verabschiedung der DS-GVO gegeben waren. Eine solche Auslegung des Art. 91 DS-GVO würde nur anderen, kleinen Religionsgemeinschaften die Möglichkeit zur Entwicklung eines eigenen Datenschutzrechts nehmen und ihnen in dieser Hinsicht religionsrechtliche Parität verweigern. Das kann nicht überzeugend sein.

26 Auch die **Praxis** im Umgang mit Art. 91 DS-GVO in zahlreichen **anderen EU-Mitgliedstaaten** hat die Inkraftsetzung und Neufassung umfassender kirchlicher Datenschutzbestimmungen ohne Weiteres und ohne Bindung an vorhan-

24 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Hrsg.), Datenschutz-Grundverordnung (BfDI-Info 6), 2. Aufl. 2016, S. 30.
25 Hense in HK-DS-GVO Art. 91 Rn. 15.

Ob die Regelungen zur Datenoffenlegungen mit Auslandsbezug gerade aufgrund ihrer engen Orientierung an Vorgaben der DS-GVO dem kirchlichen Selbstverständnis wirklich gerecht werden, sei ausdrücklich dahingestellt. 83

## § 10 Offenlegung gegenüber nicht kirchlichen und nicht öffentlichen Stellen

**(1) Die Offenlegung personenbezogener Daten gegenüber nicht kirchlichen Stellen, nicht öffentlichen Stellen oder sonstigen Empfängern ist zulässig, wenn**

**a) sie zur Erfüllung der in der Zuständigkeit der offenlegenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 6 zulassen würden, oder**

**b) der Empfänger ein berechtigtes Interesse an der Kenntnis der offenzulegenden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Offenlegung hat, es sei denn, dass Grund zu der Annahme besteht, dass durch die Offenlegung die Wahrnehmung des Auftrags der Kirche gefährdet würde.**

**(2) Die Verantwortung für die Zulässigkeit der Offenlegung trägt die offenlegende kirchliche Stelle.**

**(3) [1]In den Fällen der Offenlegung nach Absatz 1 lit. b) unterrichtet die offenlegende kirchliche Stelle die betroffene Person von der Offenlegung ihrer Daten. [2]Dies gilt nicht, wenn damit zu rechnen ist, dass sie davon auf andere Weise Kenntnis erlangt, wenn die Unterrichtung wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Person nicht geboten erscheint, wenn die Unterrichtung die öffentliche Sicherheit gefährden oder dem kirchlichen Wohl Nachteile bereiten würde.**

**(4) [1]Der Empfänger darf die offengelegten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm gegenüber offengelegt werden. [2]Die offenlegende kirchliche Stelle hat ihn darauf hinzuweisen. [3]Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Offenlegung nach Absatz 1 zulässig wäre und die offenlegende kirchliche Stelle zugestimmt hat.**

## A. Gesamtverständnis und Zweck der Norm

1 Die Norm des § 10 KDG regelt, wie in der amtlichen Überschrift zutreffend umrissen, die Offenlegung personenbezogener Daten gegenüber nicht kirchlichen und nicht öffentlichen Stellen.

## B. Verhältnis zur DS-GVO und zum BDSG

### I. Verhältnis zur KDO

2 § 10 KDG beruht weitgehend auf der Regelung zur Datenübermittlung an nicht kirchliche und nicht öffentliche Stellen in § 12 KDO.

3 Gestrichen wurde die 2003 in die KDO eingeführte Bestimmung des § 12 Abs. 1 Ziff. 2 S. 2 KDO betreffend die Zulässigkeit der Übermittlung besonderer Arten personenbezogener Daten im Sinne des § 2 Abs. 10 KDO. Zugleich wurde an den bisherigen Text als letzter Halbsatz des § 10 Abs. 1 lit. b KDG die Klausel angefügt, dass die Gefährdung der Wahrnehmung des Auftrags der Kirche der Offenlegung von Daten entgegensteht. Mit der Verarbeitung besonderer Kategorien personenbezogener Daten befasst sich nun § 11 KDG.

4 Zu den in KDO bzw. KDG jeweils verwendeten Fachbegriffen und der sonstigen Sprachregelung gelten die Ausführung zu § 9 KDG entsprechend (vgl. → KDG § 9 Rn. 4).

5 § 12 KDO war insgesamt der Norm des § 16 BDSG aF nachgebildet.[1] Jedoch fand sich nur in § 12 Abs. 3 KDO, nicht auch in § 16 Abs. 3 BDSG aF die (ebenfalls 2003 in die KDO aufgenommene) Klausel, dass eine Unterrichtung der betroffenen Person dann unterbleiben kann, wenn dies wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen nicht geboten erscheint.

### II. Verhältnis zum BDSG

6 § 25 Abs. 2 BDSG befasst sich mit der Datenübermittlung durch öffentliche Stellen an nicht öffentliche Stellen, wobei teilweise die Regelungen des § 16 BDSG aF übernommen werden. Von daher ergeben sich in etwa folgende Entsprechungen: § 25 Abs. 2 S. 1 Ziff. 1 BDSG ≈ § 10 Abs. 1 lit. a KDG; § 25 Abs. 2 S. 1 Ziff. 2 BDSG ≈ § 10 Abs. 1 lit. b KDG (ohne den oben → Rn. 3 erwähnten, gegenüber der KDO neuen Halbsatz am Ende); § 25 Abs. 2 S. 1 BDSG am Ende ≈ § 10 Abs. 4 S. 1 KDG; sowie § 25 Abs. 2 S. 2 BDSG ≈ § 12 Abs. 4 S. 2 KDG.

7 Die Regelung des § 25 Abs. 2 Ziff. 3 BDSG ist ohne Entsprechung in § 10 KDG.

8 Die Regelung des § 25 Abs. 2 S. 1 BDSG am Ende ist gegenüber § 10 Abs. 4 S. 1 KDG insofern stärker, als das staatliche Recht vom Dritten, an den Daten übermittelt werden, eine positive eigene Verpflichtung darauf verlangt,

1 Zu § 16 BDSG aF vgl. Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16; Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16; Erbs/Kohlhaas/Ambs BDSG 2003 § 6.

die Daten nur im Rahmen der Zweckbindung zu verarbeiten.[2] Das KDG spricht insoweit nur ein Verbot der zweckfremden Datenverarbeitung aus.

### III. Verhältnis zur DS-GVO

9 Mit der Schaffung des KDG hat sich der kirchliche Gesetzgeber der Auflage angenommen, die sich aus Art. 91 Abs. 1 DS-GVO am Ende ergibt, das bisherige kirchliche Datenschutzrecht gemäß KDO mit der DS-GVO in Einklang zu bringen. Daher kann im Ansatz davon ausgegangen werden, dass auch die Norm des § 10 KDG mit den Vorgaben der DS-GVO vereinbar ist (vgl. dazu auch die ergänzende Erwägung → KDG § 9 Rn. 10 mit Fn. 5).

10 Dies gilt insbesondere insoweit, inwieweit erstens KDG und BDSG übereinstimmen und dabei zweitens die Übereinstimmung der BDSG-Norm mit der DS-GVO bejaht werden kann. Diesbezüglich gilt für § 25 Abs. 2 S. 1 Ziff. 1 BDSG, dass der deutsche Gesetzgeber hier von den Öffnungsklauseln in Art. 6 Abs. 3 iVm Abs. 1 lit. e DS-GVO Gebrauch gemacht hat; und ebenso für § 25 Abs. 2 S. 1 Ziff. 3 u. S. 2 BDSG von der Öffnungsklausel in Art. 6 Abs. 4 DS-GVO.[3] Der kirchliche Gesetzgeber konnte diese Öffnungsklauseln in analoger Weise für sich nutzen (vgl. dazu auch die ergänzende Erwägung → KDG § 9 Rn. 11 mit Fn. 7).

11 Problematisch ist dagegen die Regelung des § 25 Abs. 2 S. 1 Ziff. 2 BDSG sowie folglich entsprechend die Regelung des § 10 Abs. 1 lit. b KDG, insofern hier die Öffnungsklauseln der DS-GVO nicht greifen;[4] es kommt jedoch in Betracht, eine Datenoffenlegung „an nichtöffentliche Stellen, die allein durch das überwiegende Interesse der empfangenden Stelle legitimiert wird, direkt auf Art. 6 Abs. 1 lit. f DS-GVO [zu] stützen".[5] Von daher erscheint die Auffassung vorzugswürdig, dass § 10 Abs. 1 lit. b KDG wohl nur in einer DS-GVO-konformen Auslegung anwendbar ist. Diesbezüglich dürften folgende Details beachtlich sein: Während § 10 Abs. 1 lit. b KDG das bloße Vorhandensein eines berechtigten Interesses an der Datenoffenlegung genügen lässt, verlangt Art. 6 Abs. 1 lit. f DS-GVO, dass die Datenoffenlegung zur Wahrung dieses berechtigten Interesses erforderlich ist. Während desweiteren § 10 Abs. 1 lit. b KDG das Fehlen eines schutzwürdigen Interesses der betroffenen Person am Ausschluss der Offenlegung zur Zulässigkeitsvoraussetzung einer Offenlegung erklärt, genügt nach Art. 6 Abs. 1 lit. f DS-GVO, dass die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

12 Wie bereits erwähnt, ist die Schlussklausel des § 10 Abs. 1 lit. b KDG neu und ohne Parallele im staatlichen Recht. Die Klausel führt die Interessen der Kirche, näherhin die ungefährdete Wahrnehmung ihres Auftrags, als möglichen Grund der Unzulässigkeit von Datenoffenlegungen an. Die Klausel stärkt damit das Anliegen des Schutzes personenbezogener Daten und dürfte folglich europarechtlich nicht zu beanstanden sein.

2 Vgl. speziell zu dieser Zweckbindungserklärung im staatlichen Recht Marsch in HK-BDSG § 25 Rn. 21. Mangels entsprechender Verpflichtungserklärungen „der Öffentlichkeit" kann demnach im staatlichen Rechtskreis die Veröffentlichung von Daten nicht auf § 25 Abs. 2 BDSG gestützt werden.
3 Vgl. Marsch in HK-BDSG § 25 Rn. 3.
4 Vgl. Marsch in HK-BDSG § 25 Rn. 3 u. 19.
5 Marsch in HK-BDSG § 25 Rn. 19.

13 In Spannung zur DS-GVO steht schließlich gemäß der vorstehend beschriebenen Hermeneutik wohl auch die Regelung des § 10 Abs. 4 S. 3 KDG. Denn diese Norm entspricht § 25 Abs. 2 S. 2 BDSG, welche Regelung mit Blick auf die Vorgaben der DS-GVO wohl insofern zu eng ist, als „sie auch zweckändernde Weiterverarbeitungen durch nichtöffentliche Stellen erfasst, deren Sekundärzwecke mit den Primärzwecken im Sinne von Art. 6 Abs. 4 DS-GVO vereinbar sind";[6] zugleich ist sie wohl insofern zu weit, als „sie nicht in Gänze die Vorgaben des Art. 6 Abs. 4 DS-GVO für Zweckänderungstatbestände des nationalen Rechts erfüllt".[7] Allerdings steht im Vergleich zu den Mitgliedstaaten der Europäischen Union gemäß Art. 91 Abs. 1 DS-GVO den Kirchen und Religionsgemeinschaften ein größerer Spielraum bei der „Umsetzung" der DS-GVO in das eigene Datenschutzrecht zu, insofern für diese „Umsetzung" ein „in Einklang bringen" genügt. Aus dem kritischen Befund zur Europarechtskonformität des § 25 Abs. 2 S. 2 BDSG folgt daher nicht ohne Weiteres, dass auch die Regelung des § 10 Abs. 4 S. 3 KDG mit den europarechtlichen Vorgaben unvereinbar wäre.

## C. Kommentierung

### I. Normadressat und Anwendungsbereich

14 Normadressat des § 10 KDG sind kirchliche Stellen im Sinne des § 3 Abs. 1 KDG, die personenbezogene Daten durch Offenlegung (dazu sogleich → Rn. 17) verarbeiten. Der Kreis der möglichen Adressaten einer Datenoffenlegung wird etwas umständlich mit „nicht kirchliche Stellen, nicht öffentliche Stellen oder sonstigen Empfängern" umschrieben. Damit soll einerseits zum Ausdruck gebracht werden, dass § 10 KDG auf alle Fälle von Datenoffenlegungen anwendbar ist, die nicht gegenüber kirchlichen oder öffentlichen Stellen im Sinne des § 9 KDG erfolgen. Andererseits wird mit den „sonstigen Empfängern" deutlich darauf hingewiesen, dass auch Offenlegungen an Privatleute bzw. natürliche Personen in Betracht kommen und gemäß § 10 KDG zu beurteilen sind.[8]

15 Im Gegensatz zu § 9 Abs. 1 KDG erfolgt keine räumliche Einschränkung auf Stellen oder sonstige Empfänger*innen im Geltungsbereich des § 3 KDG. Im Umkehrschluss legt dies nahe, dass § 10 KDG auch auf etwaige Datenoffenlegungen gegenüber ausländischen Stellen und sonstigen Empfänger*innen anwendbar ist. Mit Blick auf die internationale Sichtbarkeit etwaiger Veröffentlichungen von Daten im Internet sowie in sonstigen Massenmedien erscheint eine solche Auslegung auch sachgerecht.[9] Allerdings sind für Fälle mit Auslandsbezug ergänzend auch die speziellen Regelungen der §§ 39–41 KDG

6 Marsch in HK-BDSG § 25 Rn. 22.
7 Marsch in HK-BDSG § 25 Rn. 22.
8 Vgl. dazu auch Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.2–2.3.
9 Zur Vorgängernorm des § 12 KDO (2003) anderer Ansicht Hammer, Einführung in die KDO, Sekretariat der Deutschen Bischofskonferenz (Hrsg.), Datenschutz und Melderecht der katholischen Kirche 2006 (Arbeitshilfen 206), 1. Aufl. 2016, 48–103, 72: „Eine Datenübermittlung an nichtkirchliche und nichtöffentliche Stellen im Ausland ist nicht vorgesehen."

zu beachten (vgl. dazu auch → KDG § 9 Rn. 15),[10] so dass hinsichtlich der genauen Art der Datenoffenlegung nur eine „Übermittlung" in Betracht kommt (die „Übermittlung" ist eine Unterkategorie der „Offenlegung", vgl. dazu § 4 Ziff. 3 KDG sowie die Kommentierung zu → KDG § 9 Rn. 17 u. Rn. 19).

## II. Zulässigkeit der Offenlegung (Abs. 1)

§ 10 Abs. 1 KDG benennt die Voraussetzungen der Zulässigkeit der Offenlegung von Daten an nicht kirchliche und nicht öffentliche Stellen sowie an sonstige Empfänger*innen. 16

### 1. Begriff der Offenlegung

Der Begriff der Offenlegung ist in § 4 Ziff. 3 KDG legaldefiniert. Offenlegung meint daher die Datenverarbeitung durch „Übermittlung, Verbreitung oder eine andere Form der Bereitstellung" (§ 4 Ziff. 3 KDG; vgl. ferner → KDG § 9 Rn. 17 ff.). Der Begriff ist damit insgesamt weit zu verstehen und umfasst sowohl die aktive Weitergabe seitens der offenlegenden Stellen als auch den Datenabruf durch die empfangenden Stellen bzw. die sonstigen Empfänger.[11] 17

### 2. Voraussetzungen der Zulässigkeit

Die Offenlegung personenbezogener Daten an Stellen, die weder kirchlich noch öffentlich sind, sowie an sonstige Empfänger ist für zwei alternative Fallgruppen zulässig, nämlich entweder unter den Voraussetzungen gemäß § 10 Abs. 1 lit. a KDG oder unter den Voraussetzungen des § 10 Abs. 1 lit. b KDG. 18

Die erste Fallgruppe (§ 10 Abs. 1 lit. a KDG) betrifft die Offenlegung zur Erfüllung von Aufgaben der offenlegenden kirchlichen Stelle. In derartigen Fällen müssen für die Zulässigkeit der Offenlegung personenbezogener Daten kumulativ zwei Bedingungen erfüllt sein. 19

Erstens muss die Datenoffenlegung dafür erforderlich sein, dass die offenlegende kirchliche Stelle ihre Aufgaben erfüllen kann. Dieser Aspekt ist mit der Regelung aus § 9 Abs. 1 lit. a KDG vergleichbar (vgl. dazu die Kommentierung → KDG § 9 Rn. 21 f.), allerdings mit dem entscheidenden Unterschied, dass es allein auf die Aufgaben der offenlegenden Stelle ankommt, nicht jedoch auf die Aufgaben der empfangenden Stelle oder Person. Die Erforderlichkeit der Datenoffenlegung ist anhand der konkreten Aufgaben der offenlegenden Stelle zu beurteilen.[12] Die offenlegende Stelle muss sachlich und örtlich zuständig sein und die Datenoffenlegung muss der rechtmäßigen Aufgabenerfüllung dienen.[13] Die Erforderlichkeit ist (immer und nur) dann zu beja- 20

10 Für Kritik insbesondere zu § 40 Abs. 2 lit. b KDG vgl. Golland, Reformation 2.0. Umsetzung der Anforderungen der Datenschutz-Grundverordnung durch die evangelische und die katholische Kirche, Recht der Datenverarbeitung 24 (2018) 8–13, 11 f.

11 Vgl. dazu auch Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.1.

12 So zur KDO-Vorgängernorm bereits Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.6.

13 So zur KDO-Vorgängernorm bereits Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.6.

hen, wenn die offenlegende Stelle anders nicht in der Lage ist, die fragliche Aufgabe ohne Verstoß gegen die Rechtsordnung zu erfüllen.[14]

21 Zweitens muss die Datenoffenlegung ganz allgemein rechtmäßig im Sinne des § 6 KDG sein. Dieser Aspekt entspricht – ungeachtet unterschiedlicher Formulierungen – vollumfänglich der Regelung aus § 9 Abs. 1 lit. b KDG (für weitere Einzelheiten vgl. daher die Kommentierung dort → KDG § 9 Rn. 23 f.).

22 Die zweite Fallgruppe (§ 10 Abs. 1 lit. b KDG) betrifft die Offenlegung aufgrund berechtigten Interesses Dritter. In derartigen Fällen müssen für die Zulässigkeit der Offenlegung personenbezogener Daten kumulativ drei Bedingungen erfüllt sein.[15]

23 Erstens muss die empfangende Stelle oder Person ein berechtigtes Interesse an der Kenntnis der offenzulegenden Daten haben. Ein berechtigtes Interesse darf nicht mit einem rechtlichen Interesse verwechselt oder gleichgesetzt werden, wobei ein rechtliches Interesse grundsätzlich schwerer wiegt als ein nur berechtigtes Interesse und folglich stets beachtlich ist.[16] Ein berechtigtes Interesse liegt dagegen bereits dann vor, wenn Sachverhalte vorgetragen werden, die ein „Begehren in ideeller, historischer, moralischer oder wirtschaftlicher Weise belegen".[17] Das fragliche Interesse muss in der Regel ein unmittelbar oder mittelbar eigenes Interesse der empfangenden Stelle oder Person sein, um die Offenlegung zu rechtfertigen.[18] Das diesbezügliche Vorbringen muss aus objektiver Sicht nachvollziehbar sein;[19] zuständig für die diesbezügliche Beurteilung ist die offenlegende Stelle.[20] Zu den begründeten wirtschaftlichen Interessen zählt auch das Interesse an Werbung in eigener Sache, nicht jedoch der Adressenhandel.[21] Bloße Neugier stellt kein berechtigtes Interesse dar.[22]

24 Das berechtigte Interesse muss gegenüber der offenlegenden Stelle glaubhaft gemacht werden. Das bedeutet, dass kein voller förmlicher Beweis des Vortrags zum berechtigten Interesse zu erfolgen hat; es genügt eine plausible

14 So zu § 15 BDSG aF bereits Erbs/Kohlhaas/Ambs BDSG 2003 § 15 Rn. 7.
15 Wie bereits oben → Rn. 11, angesprochen wurde, ist allerdings fraglich, ob die konkrete Ausgestaltung der Norm des § 10 Abs. 1 lit. b KDG mit Art. 6 Abs. 1 lit. f DS-GVO vereinbar ist, oder für eine Konformität mit den europarechtlichen Vorgaben der DS-GVO teils extensiv, teils restriktiv ausgelegt werden muss.
16 So zu § 16 BDSG Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 10; Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 8; Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 7.
17 Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.9.
18 So zu § 16 BDSG Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 10; Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 8; Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 8.
19 Vgl. Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.9.
20 Vgl. Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.10.
21 So Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.9; differenzierter Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 8: Ein Vermarktungswunsch sei als berechtigtes Interesse an sich anerkennenswert, aber in der Abwägung mit den schutzwürdigen Interessen des Betroffenen regelmäßig ohne Durchsetzungskraft.
22 So zu § 16 BDSG Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 10; Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 8.

Erklärung, aus der sich eine überwiegende Wahrscheinlichkeit ergibt.[23] Die Bewertung insoweit hat, ebenfalls aus objektiver Sicht, durch die offenlegende Stelle zu erfolgen. Zu Beweiszwecken sollte das Vorbringen zu den berechtigten Interessen in Schriftform oder zumindest in Textform erfolgen.

Was die Vereinbarkeit des § 10 Abs. 1 lit. b KDG mit Art. 6 Abs. 1 lit. f DS- 25
GVO anbelangt (vgl. dazu → Rn. 11 sowie → Rn. 22 mit Fn. 15), so ist darauf hinzuweisen, dass die europarechtliche Regelung zusätzlich zum berechtigten Interesse auch die Erforderlichkeit der Datenoffenlegung verlangt. Trägt man diese Vorgabe im Wege einer extensiven Auslegung in § 10 Abs. 1 lit. b KDG ein, so bedeutet dies, dass trotz eines berechtigten Interesses eine Datenoffenlegung nur dann in Betracht kommt, wenn es entscheidend auf die Datenoffenlegung der angefragten kirchlichen Stelle für die Befriedigung des fraglichen Interesses ankommt. Hat die empfangende Stelle oder Person die Möglichkeit, sich die Daten selbst oder von Dritten zu beschaffen, so ist ein Tätigwerden der kirchlichen Stelle nicht veranlasst.[24]

Zweitens darf die von der Datenoffenlegung betroffene Person kein schutz- 26
würdiges Interesse an einer Nicht-Offenlegung haben. Ähnlich wie der Begriff des berechtigten Interesses zugunsten der Datenoffenlegung ist auch der Begriff des schutzwürdigen Interesses zuungunsten der Datenoffenlegung weit zu fassen.[25] Ein Interesse des bzw. der Betroffenen ist nicht erst dann beachtlich, wenn es um seine grundrechtlich geschützte Persönlichkeitssphäre geht; vielmehr können beispielsweise auch wirtschaftliche, soziale oder persönliche Belange geltend gemacht werden.[26]

Das Interesse, auf das sich der bzw. die Betroffene (tatsächlich oder hypothe- 27
tisch) beruft, muss schutzwürdig sein. Dieser auslegungsbedürftige Begriff macht nach wohl allgemeiner Auffassung eine Abwägung zwischen dem Offenlegungsinteresse der empfangenden Stelle oder Person und dem Geheimhaltungsinteresse der betroffenen Person möglich und erforderlich.[27] Die Schutzwürdigkeit des Interesses des bzw. der Betroffenen an einer Geheimhaltung seiner bzw. ihrer personenbezogenen Daten wird man regelmäßig dann verneinen können, wenn er bzw. sie selbst ein offensichtliches Interesse

23 So zu § 16 BDSG Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 10; Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 9; Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 8.

24 In diesem Sinne bereits Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.10, der vermutlich mit Blick auf einen konkreten Präzedenzfall anmerkt: „Auch ist es nicht Aufgabe kirchlicher Stellen, einem (kirchlichen oder anderen) Veranstalter von Tagungen nachträglich Daten zur Verfügung zu stellen, die dieser durch rechtzeitige Initiative, zB im Zusammenhang mit der Anmeldung, direkt beim Betroffenen hätte einholen können."

25 So zu § 16 BDSG Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 11; Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 8.

26 Vgl. Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 8.

27 Vgl. dazu Marsch in HK-BDSG § 25 Rn. 19 („überwiegende berechtigte Interesse"); ferner Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 11; Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 11; Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 8.

an der Datenoffenlegung hat; er bzw. sie in die Datenoffenlegung eingewilligt hat; oder die Daten aus allgemein zugänglichen Quellen entnommen sind.[28]

28 Die Frage des Vorliegens schutzwürdiger Interessen der betroffenen Person ist von der kirchlichen Stelle aus objektiver Sicht zu prüfen. Dazu sind von der kirchlichen Stelle alle bekannten Umstände einzubeziehen (zB Art der Daten; Möglichkeit alternativer Datenbeschaffung; Verwendung bei der empfangenden Stelle oder Person; mögliche Gefährdungen der betroffenen Person; spezifischer Konflikt der pro und contra Offenlegung im Raum stehenden Interessen; hypothetisches Verständnis der betroffenen Person für das geltend gemachte Offenlegungsinteresse).[29] Dabei dürfte es ein Gebot der Gerechtigkeit ebenso wie der Pragmatik sein, keine höheren formalen Anforderungen als hinsichtlich der Geltendmachung berechtigter Offenlegungsinteressen zu fordern. Das bedeutet, dass bereits eine überwiegende Wahrscheinlichkeit eines schutzwürdigen Interesses zu ihrer Beachtlichkeit und damit zum Ausschluss einer solchen Offenlegung führen muss.[30] Es ist ratsam, dass seitens der offenlegenden Stelle das „Ergebnis dieses schwierigen Abwägungsprozesses […] zu Beweiszwecken […] schriftlich niedergelegt“[31] wird.

29 Was die Vereinbarkeit des § 10 Abs. 1 lit. b KDG mit Art. 6 Abs. 1 lit. f DS-GVO anbelangt (vgl. dazu → Rn. 11 sowie → Rn. 22 mit Fn. 15), so ist darauf hinzuweisen, dass die europarechtliche Regelung anstatt von „schutzwürdigem Interesse“ von „Interessen oder Grundrechte und Grundfreiheiten“ der betroffenen Person spricht und für diese Interessen ausdrücklich eine Abwägung mit den Interessen an einer Datenverarbeitung vorsieht. Die Datenverarbeitung ist dann zulässig, wenn die Interessen der betroffenen Person „nicht überwiegen“. Das bedeutet für den Fall einer Gleichgewichtung der im Raum stehenden Interessen, dass eine Datenoffenlegung erfolgen kann. Die europarechtliche Regelung erweist sich somit als liberaler als die kirchliche Regelung und erleichtert im Vergleich Datenoffenlegungen, anstatt sie zu erschweren.

30 Drittens darf die Offenlegung die Wahrnehmung des Auftrags der Kirche nicht gefährden. Diese Schlussklausel ist neu und, soweit ersichtlich, ohne Vorbild in älteren staatlichen oder kirchlichen Regelungen zum Datenschutz. Da sie potenziell den Schutz personenbezogener Daten stärkt und sich aus Art. 91 Abs. 1 DS-GVO nicht das Erfordernis einer völlig mit dem weltlichen Datenschutzrecht identischen, sondern nur das Erfordernis einer mit dem weltlichen Datenschutzrecht in Einklang gebrachten, gleichwertigen kirchlichen Regelung ergibt (vgl. dazu die Nachweise → KDG § 9 Rn. 10 mit Fn. 5), die Raum für die Berücksichtigung kirchlicher Eigentümlichkeiten be-

28 So Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 11, der in der Abwägung die Schutzwürdigkeit außerdem auch dann zurücktreten lässt, wenn die Datenoffenlegung der Wahrung von Rechten Dritter oder zu Forschungszwecken dient.

29 Vgl. dazu Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.11; Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 11.

30 Wie hier Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 11; anderer Ansicht Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 8: „Für die Beeinträchtigung der schutzwürdigen Interessen des Betroffenen genügt die Glaubhaftmachung nicht.“

31 Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.11.

lässt, dürfte sie europarechtlich nicht zu beanstanden sein. Die Klausel selbst erweckt den Eindruck, ein Instrument zur quasi-willkürlichen Durchsetzung aktueller (kirchen-)politischer Interessen im Einzelfall zu sein, und dürfte im Streitfall nur schwer judiziabel sein. Denn je nach Begründung ist es auch in (scheinbar) gleichgelagerten Ausgangsfällen denkbar, dass eine Gefährdung des kirchlichen Auftrags wahlweise in der Offenlegung[32] oder der Nicht-Offenlegung[33] bestimmter personenbezogener Daten gesehen wird. Da jedoch § 10 Abs. 1 KDG zwar bei Vorliegen der dort benannten Zulässigkeitsvoraussetzungen zu einer Datenoffenlegung ermächtigt, aber die kirchlichen Stellen keineswegs dazu verpflichtet, bleiben der genaue Zweck und die Notwendigkeit dieser Schlussklausel letztlich unklar.

### III. Verantwortung für Offenlegung (Abs. 2)

31 Die Zuweisung der Verantwortung für die Offenlegung an die offenlegende kirchliche Stelle hat eine wortwörtliche Parallele in § 9 Abs. 3 S. 1 KDG. Auf die diesbezügliche Kommentierung wird verwiesen (vgl. → KDG § 9 Rn. 33 ff.).

32 Der Gesetzgeber geht augenscheinlich davon aus, dass es sich bei Offenlegungen gemäß § 10 Abs. 1 lit. b KDG jeweils nicht um automatisierte Datenabrufe handeln wird, für die ungeklärt bliebe, ob und wie die offenlegende Stelle von konkreten Offenlegungen erfährt. Käme für die Offenlegung von personenbezogenen Daten an nicht öffentliche und nicht kirchliche Stellen auch ein Datenabrufverfahren in Betracht, so wäre die Regelung des § 10 Abs. 2 KDG für die offenlegende Stelle offensichtlich unbillig, wie der Vergleich mit der insoweit differenzierteren Regelung des § 9 Abs. 3 KDG belegt (vgl. → KDG § 9 Rn. 37 ff.).

### IV. Informationspflicht (Abs. 3)

33 § 10 Abs. 3 KDG regelt die Pflicht der offenlegenden Stelle, betroffene Personen in Fällen der Offenlegung wegen überwiegender berechtigter Interessen von der Offenlegung personenbezogener Daten an nicht kirchliche und nicht öffentliche empfangende Stellen oder Personen zu unterrichten, sowie die Ausnahmen von dieser Pflicht.

#### 1. Grundsatz der Informationspflicht

34 Die Informationspflicht ist auf die zweite Fallgruppe der zulässigen Datenoffenlegung an nicht kirchliche und nicht öffentliche empfangende Stellen oder Personen, dh auf Fälle des § 10 Abs. 1 lit. b KDG beschränkt. Dahinter steht wohl zum einen die Erwägung, dass mit einer Informationspflicht auch in den Fällen des § 10 Abs. 1 lit. a KDG ein unverhältnismäßig hoher Verwaltungsaufwand seitens der kirchlichen Stelle verbunden wäre;[34] zum anderen

32 Etwa mit dem Argument der Glaubwürdigkeit durch Diskretion, ohne die der kirchliche Auftrag insgesamt in Gefahr gerät.

33 Etwa mit dem Argument der Glaubwürdigkeit durch Transparenz, ohne die der kirchliche Auftrag insgesamt in Gefahr gerät.

34 So Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 16, wobei allerdings folgender Kontext im weltlichen Rechtskreis in Erinnerung gerufen wird: „Die Übermittlung nach [§ 16 Abs. 1 Nr. 1 BDSG aF] erfolgt im Regelfall zur Durchführung von Rechtsvorschriften oder im öffentlichen Interesse."

die Überlegung, dass die Offenlegungen nach § 10 Abs. 1 lit. b KDG „in der Regel nicht vorhersehbar und einzelfallbezogen“[35] sind. Von daher stellt die Regelung einen Ausgleich dafür dar, dass die betroffene Person im Vorfeld der Datenübermittelung regelmäßig keine Möglichkeit hat, auf die Entscheidung der offenlegenden Stelle Einfluss zu nehmen. Zugleich soll daher die Informationspflicht umgekehrt die offenlegende Stelle dazu anhalten, die Prüfung der Zulässigkeitsvoraussetzungen gemäß § 10 Abs. 1 lit. b KDG sorgfältig und gewissenhaft vorzunehmen.

35 Der Gesetzgeber geht augenscheinlich davon aus, dass es sich bei Offenlegungen gemäß § 10 Abs. 1 lit. b KDG jeweils um Einzelfälle handelt, bei denen fallweise eine Prüfung und Abwägung der Interessen der empfangenden Stelle oder Person und der betroffenen Person von der offenlegenden Stelle durchführbar ist, bevor es tatsächlich zu einer Datenoffenlegung kommt. Anders gesagt: Der Gesetzgeber rechnet offenbar nicht damit, dass die empfangende Stelle oder Person Daten im Wege eines automatisierten Datenabrufs erhält. Denn im Falle von Datenabrufen der empfangenden Stelle oder Person bleibt unklar, ob und wie die offenlegende Stelle von konkreten Offenlegungen erfährt, um dann ihrer Informationspflicht aus § 10 Abs. 3 KDG nachkommen zu können.

36 Die Informationspflicht trifft die offenlegende Stelle erst (aber auch immer) dann, wenn tatsächlich eine Datenoffenlegung erfolgt ist.[36]

37 Hinsichtlich Art und Umfang der Unterrichtung der betroffenen Person sind dem geltenden kirchlichen Recht keine genaueren Vorgaben zu entnehmen. Zu § 12 Abs. 3 KDO enthielt Art. V KDO-Durchführungsverordnung die Regelung, dass die Unterrichtung schriftlich zu erfolgen hat, wobei erstens die übermittelnde Stelle nebst Anschrift; zweitens der Dritte, an den die Daten übermittelt wurden; sowie drittens die Bezeichnung der übermittelten Daten enthalten sein mussten. Es spricht nichts dagegen, die damit etablierte Praxis beizubehalten.

### 2. Weitreichende Ausnahmetatbestände

38 Die Informationspflicht gilt jedoch dann nicht, wenn einer von vier Ausnahmetatbeständen eingreift. Das Vorliegen der fraglichen Tatbestände darf seitens der offenlegenden Stelle nicht leichtfertig angenommen werden;[37] die Tatbestände sind eng auszulegen.[38]

39 Der erste Ausnahmetatbestand ist die anderweitige Kenntniserlangung der betroffenen Person von der Datenoffenlegung. Zu einer solchen anderweitigen Kenntnisnahme kommt es typischerweise dann, wenn die empfangende Stelle oder Person die betroffene Person ihrerseits von der Datenoffenlegung unterrichtet. Dabei genügt es jedoch nicht, dass die empfangende Stelle oder Person gegenüber der betroffenen Person von den offengelegten Daten Gebrauch macht; erforderlich ist auch, dass im Zuge dessen deutlich wird, dass die empfangende Stelle oder Person die fraglichen Daten durch Offenlegung

35 Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 16.
36 Vgl. BDSG Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 16; Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 10.
37 Vgl. Fachet, Datenschutz in der katholischen Kirche, KDO § 12 Rn. 2.13.
38 Vgl. Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 20.

der kirchlichen Stelle erlangt hat.[39] Dabei lässt § 10 Abs. 2 KDG eine bloße Wahrscheinlichkeit der Kenntniserlangung im Rahmen typischer Geschehensabläufe ausreichen („wenn damit zu rechnen ist, dass"). Nicht ausreichend wäre jedoch die rein hypothetische Möglichkeit, dass die betroffene Person vielleicht irgendwann irgendwie von der Datenoffenlegung der kirchlichen Stelle erfährt.[40] Der Ausnahmetatbestand greift vielmehr nur dann, wenn die Wahrscheinlichkeit einer sofortigen oder wenigstens derart zeitnahen anderweitigen Kenntniserlangung gegeben ist,[41] dass die betroffene Person noch vor der tatsächlichen Nutzung ihrer Daten durch die empfangende Stelle oder Person von einem Widerspruchsrecht[42] Gebrauch machen bzw. sich mit anderen Rechtsbehelfen gegen die Nutzung der Daten wehren kann.[43]

Der zweite Ausnahmetatbestand ist die mangelnde Gebotenheit einer Unterrichtung in Anbetracht der Art der personenbezogenen Daten und der schutzwürdigen Interessen der betroffenen Person. Dieser Ausnahmetatbestand wurde erstmals bei der Novellierung der KDO im Jahre 2003 in das kirchliche Datenschutzrecht aufgenommen. Die Regelung ist ohne Parallele in § 16 Abs. 3 S. 2 BDSG aF. Zum Begriff „schutzwürdige Interessen" der betroffenen Person gilt das oben bei → Rn. 26 ff. bereits Gesagte. Die Norm ist aufgrund ihrer subjektivierenden Formulierung („nicht geboten erscheint") datenschutzrechtlich problematisch, insofern hiermit vom Gesetzgeber nahegelegt wird, dass es gerade nicht auf eine objektivierende Betrachtungsweise, sondern allein auf die Einschätzung der offenlegenden Stelle ankommen soll. Im Sinne eines effektiven Datenschutzes kann dies nicht ohne Auswirkung auf das Tatbestandsmerkmal „Art der personenbezogenen Daten" bleiben. Der Ausnahmetatbestand kann daher wohl nur dann zum Zuge kommen, wenn die in Rede stehenden personenbezogenen Daten – jedenfalls unter Berücksichtigung der als schutzwürdig erkannten Interessen der betroffenen Person – offensichtlich trivial sind und daher ihre Offenlegung die Interessen der betroffenen Person nur bagatellhaft berührt. 40

Der dritte Ausnahmetatbestand liegt dann vor, wenn die Unterrichtung der betroffenen Person die öffentliche Sicherheit gefährden würde. Die letztlich aus § 16 Abs. 3 S. 2 BDSG aF übernommene Regelung hat in der weltlichen Rechtssphäre ihren Sitz im Leben in solchen Fällen, in denen der Staat private Arbeitgeber*innen über Sicherheitsbedenken oder laufende Ermittlungen gegen Arbeitnehmer*innen informiert.[44] Dass die Kirche auf Initiative einer nicht öffentlichen Stelle mit dieser personenbezogene Daten teilt und die öf- 41

39 Vgl. Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 20.
40 Vgl. Erbs/Kohlhaas/Ambs BDSG 2003 § 16 Rn. 10.
41 Vgl. Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 17; Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 20.
42 Ein solches Widerspruchsrecht regeln etwa § 23 KDG; § 36 BDSG. Insofern in den einschlägigen Fällen eine Datenoffenlegung an nicht kirchliche und nicht öffentliche Stellen vorliegt, dürften die genannten Normen allerdings (als Anspruchsgrundlage gegenüber der empfangenden Stelle oder Person) unanwendbar sein.
43 Vgl. Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 17.
44 Vgl. Klug/Körffer/Schomerus in Gola/Schomerus, 10. Aufl. 2010, BDSG § 16 Rn. 17; Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 21.

fentliche Sicherheit gefährdet wäre, wenn die von der Offenlegung betroffene Person hiervon erfährt, ist wohl nur in extremen Sonderfällen denkbar.[45]

42 Der vierte Ausnahmetatbestand wäre dann gegeben, wenn die Unterrichtung dem kirchlichen Wohl Nachteile bereiten würde. Auch diese Regelung hat ihr gedankliches Vorbild letztlich in § 16 Abs. 3 S. 2 BDSG aF, der insoweit allerdings auf Nachteile für das Wohl des Bundes oder eines Landes abstellte. Erneut lässt sich die Frage stellen, ob und welchen Sitz im Leben diese Regelung haben kann: In welchen Situationen kommt es in Betracht, dass die Offenlegung von personenbezogenen Daten gegenüber einem Dritten, der die Kirche danach fragt, für die Kirche nicht nachteilig ist, während zugleich die Unterrichtung der betroffenen Person vom Vorgang der Offenlegung nachteilig ist?[46] Die Norm ist daher datenschutzrechtlich problematisch. Eine Auslegung, wonach die Nachteiligkeit der Unterrichtung immer dann zu bejahen ist, wenn die Zulässigkeit der Offenlegung unklar, dh die korrekte Prüfung und Abwägung der im Raum stehenden Interessen gemäß § 10 Abs. 1 lit. b zweifelhaft oder gar fehlerhaft ist, dürfte sich wohl verbieten. Denn eine solche Auslegung stünde in klarem Widerspruch zum generellen Sinn und Zweck des § 10 Abs. 3 KDG, die betroffene Person über die Offenlegung von Daten zu informieren.

## V. Zweckbindung (Abs. 4)

43 § 10 Abs. 4 schärft den Grundsatz der Zweckbindung[47] bei der Verarbeitung personenbezogener Daten ein.

44 Dabei ist § 10 Abs. 4 S. 1 wortgleich mit § 9 Abs. 4 S. 1 KDG; auf die diesbezügliche Kommentierung kann verwiesen werden → KDG § 9 Rn. 41.

45 § 10 Abs. 4 S. 2 KDG bestimmt, dass die offenlegende Stelle die empfangende Stelle oder Person auf die strikte Zweckbindung bei der Verarbeitung hinzuweisen hat. Demgegenüber verlangt § 25 Abs. 2 S. 1 BDSG am Ende, dass sich bei einer Datenübermittlung an nicht öffentliche Stellen zuvor der Dritte gegenüber der übermittelnden öffentlichen Stelle dazu verpflichtet hat, bei der eigenen Datenverarbeitung die Zweckbindung zu beachten. Die Unterschiede zwischen beiden Regelungen sind hinsichtlich ihrer datenschutzrechtlichen Auswirkungen gravierend. Zum einen macht es gewiss einen psychologischen Unterschied, ob die empfangende Stelle lediglich passiv einen Hinweis der offenlegenden Stelle zur Kenntnis nehmen muss, oder ob sie aktiv eine Verpflichtungserklärung abzugeben hat. Zum anderen verunmöglicht es die staatliche Regelung, die Veröffentlichung personenbezogener Daten rechtlich auf § 25 Abs. 2 BDSG zu stützen, weil „die Öffentlichkeit" gegenüber der übermittelnden Stelle keine entsprechende Verpflichtungserklärung

45 Ob derartige Fälle aber undenkbar sind und daher objektiv kein Regelungsbedürfnis gegeben ist, sei hier bewusst offengelassen. Näherungsweise denkbar – aber kein Fall des § 10 Abs. 1 lit. b KDG – wäre beispielsweise die Situation, dass in einem kirchlichen Eheverfahren einer psychisch labilen Partei verheimlicht wird, dass die Verfahrensakte einem*r externen Sachverständigen zur fachwissenschaftlichen Stellungnahme offengelegt wurde, wenn und weil im Falle einer diesbezüglichen Unterrichtung der besagten Partei mit einem Amoklauf gerechnet werden muss.

46 So bereits mit Blick auf die staatliche Norm Wedde in Däubler/Klebe/Wedde/Weichert, 4. Aufl. 2014, BDSG § 16 Rn. 22.

47 Vgl. dazu auch Art. 5 lit. b DS-GVO.

### B. Verhältnis zur DS-GVO und zum BDSG

2 § 35 KDG korrespondiert mit Art. 35 DS-GVO. Auch § 67 BDSG enthält eine Regelung zur Datenschutz-Folgenabschätzung. Dies ist allerdings in Teil 3 des BDSG geregelt, welcher der Umsetzung der JI-Richtlinie 2016/680 dient. Dieser bezieht sich lediglich auf die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen.

### C. Kommentierung

3 Die Auslegung von Art. 35 DS-GVO ist unter Berücksichtigung folgender punktueller Abweichungen der Normtexte auf § 35 KDG übertragbar:

4 § 35 KDG sieht zusätzlich in Abs. 3 die Möglichkeit der Vorlage zur Datenschutzaufsicht zwecks Stellungnahme vor. Eine Konsultationspflicht bei tatsächlichem Bestehen eines hohen Risikos gemäß § 35 Abs. 11 KDG findet sich außerdem nur im KDG.

5 Gemäß Art. 35 Abs. 4 DS-GVO soll die Aufsichtsbehörde eine Liste der Fälle von Absatz 1 veröffentlichen. Dies soll gemäß § 35 Abs. 5 KDG auch die kirchliche Datenschutzaufsicht. Dabei soll sich diese an den Listen der Aufsichtsbehörden des Bundes und der Länder orientieren, § 35 Abs. 6 KDG.

6 Zudem besteht eine Ausschlussregelung in § 35 Abs. 9 KDG für den Fall, dass schon bei der Setzung der kirchenrechtlichen Rechtsgrundlage für die Verarbeitung eine Folgenabschätzung erfolgte. Art. 35 Abs. 10 DS-GVO enthält zwar eine ähnliche Vorschrift für den Fall des Unions- oder mitgliedsstaatlichen Rechts, allerdings folgt daraus nicht direkt der Ausschluss. Wenn es nach dem Ermessen der Mitgliedsstaaten erforderlich ist, gelten die Absätze 1 bis 7 und eine Folgenabschätzung wird durchgeführt, Art. 35 Abs. 10 aE DS-GVO.

7 Auch Art. 35 DS-GVO enthält gegenüber § 35 KDG Ergänzungen. So stellt Art. 35 Abs. 7 Nr. 4 DS-GVO im Rahmen der Angabe des Mindestinhaltes einer Folgenabschätzung heraus, dass den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird. Auch die Einhaltung nach Art. 40 DS-GVO genehmigter Verhaltensregeln soll gemäß Art. 35 Abs. 8 DS-GVO berücksichtigt werden.

## Abschnitt 3 Betrieblicher Datenschutzbeauftragter

### § 36 Benennung von betrieblichen Datenschutzbeauftragten

**(1) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. a) benennen schriftlich einen betrieblichen Datenschutzbeauftragten.**

**(2) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. b) und c) benennen schriftlich einen betrieblichen Datenschutzbeauftragten, wenn**

**a) sich bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen,**

**b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmä-**

**ßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder**

**c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 besteht.**

**(3) Für mehrere kirchliche Stellen im Sinne des § 3 Absatz 1 kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer betrieblicher Datenschutzbeauftragter benannt werden.**

**(4) [1]Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des betrieblichen Datenschutzbeauftragten. [2]Die Benennung von betrieblichen Datenschutzbeauftragten nach Absatz 1 ist der Datenschutzaufsicht anzuzeigen.**

**(5) [1]Der betriebliche Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags oder einer sonstigen Vereinbarung erfüllen. [2]Ist der betriebliche Datenschutzbeauftragte Beschäftigter des Verantwortlichen, finden § 42 Absatz 1 Satz 1 2. Halbsatz und § 42 Absatz 1 Satz 2 entsprechende Anwendung.**

**(6) Zum betrieblichen Datenschutzbeauftragten darf nur benannt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.**

**(7) [1]Zum betrieblichen Datenschutzbeauftragten soll derjenige nicht benannt werden, der mit der Leitung der Datenverarbeitung beauftragt ist oder dem die Leitung der kirchlichen Stelle obliegt. [2]Andere Aufgaben und Pflichten des Benannten dürfen im Übrigen nicht so umfangreich sein, dass der betriebliche Datenschutzbeauftragte seinen Aufgaben nach diesem Gesetz nicht umgehend nachkommen kann.**

**(8) Soweit keine Verpflichtung für die Benennung eines betrieblichen Datenschutzbeauftragten besteht, hat der Verantwortliche oder der Auftragsverarbeiter die Erfüllung der Aufgaben nach § 38 in anderer Weise sicherzustellen.**

## A. Gesamtverständnis und Zweck der Norm

1 Kapitel 4 Abschnitt 3 des Gesetzes über den Kirchlichen Datenschutz (KDG) regelt die Benennung (§ 36), die Rechtsstellung (§ 37) sowie die Aufgaben (§ 38) des betrieblichen Datenschutzbeauftragten (im Folgenden: bDSB). Die in § 36 Abs. 1 bis Abs. 3 genannten kirchlichen Stellen sind dazu angehalten, durch die Benennung betrieblicher Datenschutzbeauftragter dem kirchlichen Datenschutz in ihrem Verantwortungsbereich zu optimaler Wirksamkeit zu verhelfen. Der bDSB kontrolliert die Einhaltung der datenschutzrechtlichen Bestimmungen, unterstützt und berät den Verantwortlichen. Funktional ergänzt er damit auch die Datenschutzaufsicht, ohne indes als deren „verlängerter Arm oder Hilfsorgan" tätig zu werden.[1] Entsprechend der europarechtlichen Vorgabe des Art. 37 DS-GVO geht es bei § 36 KDG um die Verankerung des datenschutzrechtlichen Konzepts der Selbstkontrolle des Verantwortlichen für die Datenverarbeitung. Ein maßgeblicher Regelungshintergrund der Bestellung eines bDSB ist dabei die gesetzgeberische Vorstellung, dass die große Sachnähe eines mit der Datenverarbeitung und dem Schutz personenbezogener Daten vertrauten Beauftragten dazu beitragen kann, Verletzungsrisiken zu minimieren und Verarbeitungsvorgänge und -strukturen datenschutzfreundlich zu gestalten und weiterzuentwickeln.[2] Auch Erwägungsgrund (im Folgenden: EG) 97 zur DS-GVO erachtet die Unterstützung des Verantwortlichen durch eine weitere Person, „die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt", für sinnvoll. Diese Unterstützung kann durch einen internen oder externen Beauftragten geleistet werden,[3] der europäische Gesetzgeber fordert jedoch explizit eine „völlige Unabhängigkeit" des Datenschutzbeauftragten.

## B. Übernahme und eigene Akzentuierungen im Verhältnis zur DS-GVO / zum BDSG

2 Art. 37 DS-GVO enthält die grundlegenden Regelungen zur Benennung von Datenschutzbeauftragten für den öffentlichen und den nicht-öffentlichen Bereich.[4] Es obliegt dem kirchlichen Gesetzgeber, eine vergleichbare Regelung zu schaffen bzw. bestehende Regeln mit den Vorgaben der DS-GVO „in Einklang" zu bringen, s. Art. 91 Abs. 1 DS-GVO.[5] Um einen normativen Gleich-

1 Drewes in NK-DatenschutzR DS-GVO Art. 37 Rn. 4; Kort, Was ändert sich für Datenschutzbeauftragte, Aufsichtsbehörden und Betriebsrat mit der DS-GVO ZD 2017, 3 (7).
2 Helfrich in HK-DS-GVO Art. 37 Rn. 5.
3 Kremer in Laue/Kremer Neues DatenschutzR § 6 Rn. 17.
4 Drewes in NK-DatenschutzR DS-GVO Art. 37 Rn. 1.
5 Zur Problematik der Konvergenz der religionseigenen Regelungen mit der DS-GVO siehe Hense in HK-DS-GVO Art. 91 Rn. 17 ff.; eher kritisch zur Frage, ob die Konvergenz gelungen ist: Hoeren, Kirchlicher Datenschutz nach der Datenschutzgrundverordnung NVwZ 2018, 373 (374 f.). Auf den Umstand, dass Kirchenautonomie im Datenschutzbereich nicht mit einer Abschreibepflicht staatlicher Regelungen gleichzusetzen ist, weist bereits Isensee, Diskussionsbeitrag, in: Joseph Krautscheidt/Heiner Marré, Essener Gespräche zum Thema Staat und Kirche, Bd. 15, Münster 1981, S. 142, hin.

klang mit den europäischen Vorgaben herzustellen und die ehemals in den §§ 20, 21 KDO bestehenden Regelungen zum bDSB fortzuentwickeln, wurde ein dreigliedriger Aufbau der Regelungskomplexe Benennung, Rechtsstellung und Aufgabenbereich des bDSB gewählt.

3 § 36 Abs. 1 und Abs. 2 KDG orientieren sich an Art. 37 Abs. 1 DS-GVO, übertragen zugleich aber auch Regelungselemente der alten § 20 Abs. 1 und 2 KDO in das neue Gesetz (dazu unten → Rn. 34 ff.). § 20 Abs. 1 KDO aF wird – vom Anwendungsbereich her nunmehr begrenzt auf die Diözesen, die Kirchengemeinden, die Kirchenstiftungen und die Kirchengemeindeverbände – zum neuen § 36 Abs. 1 KDG. Damit sind die wesentlichen, in der Regel mit öffentlich-rechtlichem Status nach staatlichem Recht ausgestatteten[6] kirchlichen Rechtsträger normativ auf das Tatbestandsmerkmal „Behörde oder öffentliche Stelle" iSv Art. 37 Abs. 1 lit. a DS-GVO hin ausgerichtet worden. Die Regelung einer verpflichtenden schriftlichen Benennung eines bDSB für kirchliche Stellen iSd § 3 Abs. 1 lit. b und c KDG, sofern eine regelmäßige Mindestgrenze von zehn Personen überschritten wird, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, entspricht im Wesentlichen § 20 Abs. 2 KDO aF sowie § 38 Abs. 1 S. 1 BDSG für den bDSB nicht-öffentlicher Stellen, allerdings ohne den Hinweis auf die „automatisierte" Verarbeitung. § 36 Abs. 2 lit. b und lit. c KDG entsprechen nahezu wortlautidentisch Art. 37 Abs. 1 lit. b und lit. c DS-GVO.

4 § 36 Abs. 3 KDG trifft eine vergleichbare Regelung zu Art. 37 Abs. 2 und Abs. 3 DS-GVO bzw. § 5 Abs. 2 BDSG (gemeinsamer betrieblicher Datenschutzbeauftragter, s. a. § 20 Abs. 3 S. 3 KDO aF), § 36 Abs. 4 KDG (Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten und Mitteilung an die Aufsichtsbehörde) entspricht Art. 37 Abs. 7 DS-GVO bzw. § 5 Abs. 5 BDSG.

5 § 36 Abs. 5 S. 1 KDG entspricht Art. 37 Abs. 6 DS-GVO bzw. § 5 Abs. 4 BDSG, erweitert diesen allerdings in Satz 2 um einen Verweis auf § 42 Abs. 1 S. 1 2. Hs. sowie Abs. 1 S. 2 KDG, sofern der bDSB Beschäftigter des Verantwortlichen ist. Die Regelungstechnik entspricht dem datenschutzrechtlichen Vorbild von § 20 Abs. 8 iVm § 16 Abs. 1 KDO aF Da die Frage nach der Zulässigkeit einer befristeten Aufgabeübertragung und einer möglichen Wiederbestellung vom europäischen Verordnungsgeber nicht geregelt wurde (dazu unten → Rn. 13), ist der kirchliche Gesetzgeber nicht daran gehindert, eigenständig Konkretisierungen vorzunehmen.

6 § 36 Abs. 6 KDG gibt § 20 Abs. 3 S. 1 KDO wörtlich wieder. Die Regelung entspricht inhaltlich Art. 37 Abs. 5 DS-GVO, der allerdings die in EG 97 zur Verordnung genannten Tatbestandsmerkmale „auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benennt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt" normiert. Eine materiellrechtliche Abweichung ist mit der Übernahme der bekannten und bewährten Formulierung in § 36 Abs. 6 KDG nicht verbunden, das Tatbestandsmerkmal „Fachkunde" schließt das verordnungsrechtlich verwandte Merkmal „Fachwissen" mit ein.

6 Zum Körperschaftsstatus siehe: Unruh, Religionsverfassungsrecht, 4. Aufl., Baden-Baden 2018, § 9. Umfassend: Magen, Kirchen und andere Religionsgemeinschaften als Körperschaften des öffentlichen Rechts, in HdbStKirchR[3] § 27 (i. E.).

7 § 36 Abs. 7 KDG findet keine Entsprechung in Art. 37 DS-GVO, überträgt mit Blick auf die Vermeidung von Interessenkonflikten bei der Benennung einer geeigneten Person zum bDSB allerdings den Regelungsgedanken von Art. 38 Abs. 6 S. 2 DS-GVO in den Wortlaut der Norm. Auch § 36 Abs. 8 KDG findet kein normatives Vorbild in Art. 37 DS-GVO, verschärft jedoch das bereits in § 20 Abs. 9 KDO aF enthaltene Gebot, bei Fehlen der Voraussetzungen für die verpflichtende Benennung eines Datenschutzbeauftragten auf eine anderweitige Erfüllung der Aufgaben nach § 38 KDG hinzuwirken. § 36 Abs. 8 KDG spricht mit der Formulierung „hat … in anderer Weise sicherzustellen" eine besondere Verpflichtung des Verantwortlichen aus, geeignete Alternativen zu eruieren, um dem kirchlichen Datenschutz zu möglichst optimaler Wirksamkeit zu verhelfen. § 20 Abs. 9 KDO aF war durch die Formulierung „kann … in anderer Weise geregelt werden" wesentlich zurückhaltender.

8 Insgesamt hat die Pflicht zur Bestellung eines bDSB durch das KDG eine spürbare Ausweitung erfahren.[7] War die Benennung eines solchen etwa für den Bereich der Pfarreien in § 20 Abs. 1 iVm § 1 Abs. 2 Ziff. 1 KDO als „Kann"-Vorschrift ausgestaltet, so sieht § 36 Abs. 1 iVm § 3 Abs. 1 lit. a KDG die Pflicht zur Benennung vor. Die Aufnahme eines separaten Regelungsabschnitts zum bDSB in die DS-GVO bewirkt auch eine erhebliche verordnungsrechtliche Erhöhung dieses Berufsbildes.

## C. Kommentierung

### I. Der Rechtsakt der Benennung

#### 1. Begriff

9 Das KDG versteht gem. § 4 Ziff. 23 unter dem „betrieblichen" Datenschutzbeauftragen ausschließlich den vom Verantwortlichen oder vom Auftragsverarbeiter benannten Datenschutzbeauftragten. Diese Legaldefinition findet kein Vorbild in Art. 4 DS-GVO, wurde in Anbetracht der Bedeutung des bDSB, der Normierung in §§ 20, 21 KDO sowie der eindeutigen Abgrenzung zum Diözesandatenschutzbeauftragten in §§ 42 ff. KDG jedoch für sinnvoll erachtet.

#### 2. Schriftform der Benennung

10 § 36 Abs. 1 und 2 KDG normieren die **Schriftform** der Benennung der bDSB. Dies dient nicht nur dem Beweisinteresse des Benannten, sondern zugleich der Erfüllung der Nachweispflichten des Verantwortlichen, wie sie sich zB aus § 7 Abs. 2 KDG ergeben. Die DS-GVO kennt eine besondere Form der Benennung nicht, die vormals in § 4 f Abs. 1 S. 1 BDSG-alt normierte Schriftform iSv § 126 BGB ist im novellierten § 5 BDSG ersatzlos entfallen.[8] Aus dem Schriftformerfordernis wird abgeleitet, dass in der Benennungsurkunde Aufgabe und organisatorische Stellung zu konkretisieren sind.[9] Dieser Ansicht ist für den kirchlichen Bereich auch mit Blick auf die Vorgabe von § 36

7 Ullrich, Neue Datenschutzregelung für die Einrichtungen der katholischen Kirche, ZMV 2018, 114 (117).
8 Kremer in Laue/Kremer Neues DatenschutzR § 6 Rn. 6; Gola in Gola/Heckmann BDSG § 5 Rn. 7.
9 Reinhard, Die neue Rolle des betrieblichen Datenschutzbeauftragten ArbRB 2017, 317 (318).

Abs. 7 S. 2 KDG zuzustimmen. Diese aufgabenbezogene Einschätzung kann nur geleistet werden, wenn die Aufgabenbereiche eindeutig konturiert sind. Der Mangel der Schriftform macht die Benennung unwirksam.[10]

### 3. Zustimmung zur Benennung

Umstritten ist, ob der bDSB der Benennung zustimmen bzw. das Schriftstück gegenzeichnen muss. § 36 KDG sieht eine solche Gegenzeichnung des Benennungsaktes zwar nicht expressis verbis vor, dennoch ist sie aus Gründen der Beweisbarkeit zu empfehlen. Zu unterscheiden ist dabei zwischen dem internen und dem externen bDSB:[11] der externe Datenschutzbeauftragte nimmt den Auftrag im Wege seiner Dienstleistungsvereinbarung an und muss nicht nochmals gesondert seine Zustimmung gegenüber dem Verantwortlichen zum Ausdruck bringen. Liegt der Benennung jedoch ein Arbeitsverhältnis zugrunde, hängt es von der Reichweite des Direktionsrechts des Arbeitgebers sowie der zugrunde liegenden Aufgabenbeschreibung ab, ob der Arbeitgeber die besonderen Aufgaben des betrieblichen Datenschützers einseitig zuweisen kann. Im kirchlichen Bereich dürften im Regelfall die Benennung (wie auch die Abberufung als actus contrarius, sofern keine Teilkündigung vorliegt) für den Beschäftigten des Verantwortlichen eine Änderung seines Arbeitsvertrages bedeuten,[12] die (auch konkludent)[13] vom zukünftigen bzw. ehemaligen bDSB angenommen werden muss.[14] 11

### 4. Natürliche und juristische Person als betriebliche Datenschutzbeauftragte

Ob der bDSB eine *natürliche* Person sein muss oder auch eine *juristische* Person sein darf, ist umstritten.[15] Nach teilweise vertretener Ansicht könne nur eine natürliche Person über „Fachkunde" und „Zuverlässigkeit" (vgl. § 36 Abs. 6 KDG) bzw. über „Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren" iSv EG 97 der Richtlinie verfügen.[16] Nach anderer Auffassung tritt diese Engführung in den staatlichen Datenschutzge- 12

10 Zur alten Rechtslage nach § 20 KDO: Ausführungen zum Betrieblichen Datenschutzbeauftragten nach § 20 KDO (2014), Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland in den Sitzung vom 19./20. Oktober 2016 in Magdeburg, S. 1 (6), online abrufbar unter: https://www.katholisches-datenschutzzentrum.de/infothek/ (letzter Zugriff: Juni 2020). Nunmehr: Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands (Hrsg.), Betrieblicher Datenschutzbeauftragter nach dem Kirchlichen Datenschutzgesetz (KDG), Praxishilfe 2, Dortmund 2017, S. 3.

11 Zum Folgenden: Reinhard ArbRB 2017, 317 (318).

12 BAG NJW 2007, 2507 (2508); BAG NJW 2011, 476 (476 Rn. 12).

13 BAG NJW 2011, 476 (476 Rn. 12).

14 Ausführungen zum Betrieblichen Datenschutzbeauftragten nach § 20, S. 1 (6).

15 Gola in Gola/Heckmann BDSG § 5 Rn. 14; Sörup/Batman, Der betriebliche Datenschutzbeauftragte – Fragen über Fragen?, ZD 2018, 553 mwN; Knopp, Dürfen juristische Personen zum betrieblichen Datenschutzbeauftragten bestellt werden?, DuD 2015, 98 ff.; Franck/Reif, Pluralistische Datenschutzkontrolle. Datenschutzbeauftragte, Stellvertreter, Hilfspersonal und mehr ZD 2015, 405 (407); Baumgartner/Hansch, Der betriebliche Datenschutzbeauftragte. Best Practices und offene Fragen ZD 2019, 99 (102).

16 Drewes in NK-DatenschutzR DS-GVO Art. 37 Rn. 49. Nach Gola, Der externe Datenschutzbeauftragte, RDV 2019, 157 (160 mwN), halten die staatlichen Datenschutzaufsichtsbehörden auch nach Inkrafttreten der DS-GVO mehrheitlich an ihrer Ablehnung einer juristischen Person als bDSB fest.

setzen nicht so eindeutig hervor, so dass grundsätzlich auch eine Aufgabenübertragung auf juristische Personen für möglich gehalten wird.[17] § 20 KDO aF hat sich zu dieser Frage nicht expressis verbis verhalten, wenngleich sich § 20 Abs. 6 KDO („Kündigung seines Arbeitsverhältnisses") und § 20 Abs. 7 KDO, der dem bDSB ua einen Kostenübernahmeanspruch für Fort- und Weiterbildungskosten „zur Erhaltung der zur Erfüllung seiner Aufgabe erforderlichen Fachkunde" gewährte, wohl eher für das Erfordernis einer natürlichen Person heranziehen lassen.[18] Auch § 36 KDG spricht nur allgemein vom „betrieblichen" DSB. Aus § 36 Abs. 5 S. 1 KDG ergibt sich indes, dass selbiger entweder „Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters" sein kann oder seine Aufgaben „auf der Grundlage eines Dienstleistungsvertrags oder einer sonstigen Vereinbarung erfüllen" kann. Diese tatbestandliche Erweiterung (und auch Klarstellung) im Vergleich zur Vorgängernorm spricht für die Zulässigkeit der Benennung auch juristischer Personen zum „betrieblichen" DSB.[19] Nicht nur können deren *Beschäftigte* sehr wohl über Fachkunde und Zuverlässigkeit verfügen. Auch würde der Wirksamkeit des kirchlichen Datenschutzes nicht dadurch geholfen, dass gerade kleinere kirchliche Dienststellen und Einrichtungen nicht rechtzeitig oder möglicherweise überhaupt keine geeigneten Kandidaten für den Posten des bDSB gewinnen könnten. Ganz grundsätzlich kann die Beauftragung externer Dritter aufgrund größeren Know-Hows sowie der auch unternehmensrechtlich sichergestellten Unabhängigkeit und Weisungsfreiheit durchaus im Interesse des Verantwortlichen liegen.[20]

### 5. Befristungsfragen

13 Der Frage nach der rechtlichen Zulässigkeit einer befristeten Benennung zum bDSB begegnet § 36 Abs. 5 S. 2 KDG – für den Fall, dass der bDSB Beschäftigter des Verantwortlichen ist – mit einem Verweis auf § 42 Abs. 1 S. 1, 2. Hs. sowie § 42 Abs. 1 S. 2 KDG. Somit wird der bDSB für die Dauer von mindestens vier, höchstens acht Jahren bestellt. Eine mehrmalige erneute Bestellung ist zulässig. Eine gleichsam „indirekte" Befristung kann mit Blick auf das zugrunde liegende Arbeitsverhältnis vorliegen, sofern dieses seinerseits noch nicht entfristet wurde. Dann endet mit dem Auslaufen des Beschäftigungsverhältnisses zugleich auch die Benennung zum bDSB.[21] Die hier vorgesehene Mindestbestellungsdauer wird in der Praxis voraussichtlich dazu führen, dass der zuständige Dienstgeber bei (mit oder ohne Sachgrund) befristeten Arbeitsverhältnissen von der Benennung zum bDSB absehen wird. Für

17 Knopp DuD 2015, 98 (99, 102); Simitis in Simitis BDSG § 4 f Rn. 48.
18 Zur Zulässigkeit einer juristischen Person als betrieblichem Datenschutzbeauftragten bereits nach alter Rechtslage: Ausführungen zum Betrieblichen Datenschutzbeauftragten nach § 20 KDO, S. 1 (3).
19 I.E. auch Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands (Hrsg.), Praxishilfe 2, Dortmund 2017, S. 5. Ausdrücklich hat jüngst etwa das Bistum Aachen eine Wirtschaftsprüfungsgesellschaft zum betrieblichen Datenschutzbeauftragten für das Bischöfliche Generalvikariat und die seiner Aufsicht unterstehenden Einrichtungen in Trägerschaft des Bistums bestellt, KA 2019, S. 301. Das Bistum Görlitz hat ebenfalls eine GmbH als (gemeinsamen) betrieblichen Datenschutzbeauftragten für die *Kirchengemeinden* bestellt, Abl. 2019, Nr. 10, S. 7.
20 Vgl. Sörup/Batman ZD 2018, 553.
21 Vgl. Gola in Gola/Heckmann BDSG § 5 Rn. 17.

den externen Datenschutzbeauftragten gilt der Verweis in § 36 Abs. 5 S. 2 KDG hingegen nicht, so dass sowohl eine sachlich begründete und kürzer als 4 Jahre bemessene Benennung als auch eine unbefristete Aufgabenübertragung zulässig sind.[22] Die Aufgabenübertragung sollte jedoch nicht zu eng befristet sein, gerade, um die Unabhängigkeit des externen Datenschutzbeauftragten nicht zu gefährden. Eine Befristung von zwei Jahren dürfte als Untergrenze der Benennung sicherlich geboten sein.

### 6. Publizitätserfordernisse

14 Der Verantwortliche bzw. der Auftragsverarbeiter haben gem. § 36 Abs. 4 KDG die **Kontaktdaten** des bDSB zu veröffentlichen und die Benennung der Datenschutzaufsicht anzuzeigen. Weder das KDG, noch die DS-GVO oder das BDSG enthalten Hinweise auf die Form und den näheren Informationsumfang. In der Kommentarliteratur zum staatlichen Datenschutzrecht werden neben der Post- bzw. der Dienstanschrift noch die E-Mail-Adresse und die Telefonnummer für erforderlich gehalten, nicht hingegen der Name des Datenschutzbeauftragten.[23]

15 Wenngleich sich aus EG 58 zur DS-GVO wohl eine Präferenz für eine elektronische Publikation ergibt, dürfte die Ausprägung der **Veröffentlichungspflicht einrichtungsspezifisch für den jeweiligen Einzelfall** auszulegen sein. Eine möglichst breite Streuung der Kontaktdaten des Datenschutzbeauftragten ist jedoch anzustreben. Für kirchliche Stellen im Sinne des § 3 Abs. 1 lit. a und b KDG kommt sicherlich eine Veröffentlichung im jeweiligen Amtsblatt, einschlägigen Verbandspublikationen sowie auf der jeweiligen Homepage in Betracht. Zugleich ist eine Veröffentlichung auch dienststellenintern – via Intranet oder Rundmail – sinnvoll. Für kleinere Einrichtungen und Vereine dürften auch Aushänge und Rundschreiben in Betracht kommen. Nicht verlangt werden kann die Schaffung eines gesonderten Publikationsorgans bzw. das Erstellen einer Homepage, falls dies die technischen, personellen und finanziellen Mittel einer Einrichtung überfordern würde.

16 Die **Mitteilung im Sinne des § 36 Abs. 4 S. 2 KDG** kann (fern)mündlich oder schriftlich gegenüber der zuständigen Aufsichtsstelle erklärt werden. Unter Dokumentationsgesichtspunkten empfiehlt sich eine Mitteilung mindestens in Textform (§ 126 b BGB).[24] Die Datenschutzaufsicht kann die kirchlichen Stellen iSv § 3 KDG dabei logistisch-meldetechnisch unterstützen.[25] So stellt

22 Dazu und zum Folgenden: Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands (Hrsg.), Praxishilfe 2 Dortmund 2017, S. 5 f.

23 Gola in Gola/Heckmann BDSG § 5 Rn. 21; Kremer in Laue/Kremer Neues DatenschutzR § 6 Rn. 20; Drewes in NK-DatenschutzR DS-GVO Art. 37 Rn. 68, nach dem die Veröffentlichung des Namens allerdings alleine schon unter Vertrauensgesichtspunkten sinnvoll ist.

24 Kremer in Laue/Kremer Neues DatenschutzR § 6 Rn. 19.

25 So auch im staatlichen Bereich, s. Gola in Gola/Heckmann BDSG § 5 Rn. 21.

zB das Katholische Datenschutzzentrum Dortmund über seine Homepage ein Online-Meldeformular zur Verfügung.[26]

### 7. Besondere subjektive Benennungsvoraussetzungen

17 § 36 Abs. 6 KDG fordert eine zur Erfüllung seiner Aufgaben – *vor* der Benennung bestehende[27] – besondere Fachkunde und Zuverlässigkeit. Die hier auftretenden unbestimmten Rechtsbegriffe sind aus bestimmten Bereichen der staatlichen Rechtsordnung bekannt, etwa aus dem Wirtschaftsverwaltungs-, insbesondere dem Gewerberecht (§ 35 GewO) oder auch dem Waffenrecht (§§ 4, 7, 21, 22 WaffG). Sie sind durch Rechtsprechung und Literatur hinreichend konkretisiert worden und können auch im datenschutzrechtlichen Kontext nach wie vor wertvolle Auslegungshinweise geben,[28] dies umso mehr, als der kirchliche Gesetzgeber auf diese – aus § 20 Abs. 3 KDO aF übernommene – Formulierung zurückgreift und damit von der Vorgabe aus Art. 37 Abs. 5 DS-GVO abweicht. „Sachkunde" im waffenrechtlichen Kontext wird einzelfallspezifisch verstanden, gerade *nicht* generalisierend. Art und Umfang der waffenrechtlichen Sachkunde müssen mit dem jeweiligen Grund für den Waffenbesitz korrespondieren.[29] Neben Rechts- und Technikkenntnissen bedarf es auch praktischer Fähigkeiten.

18 Mit Blick auf die vor allem gewerberechtlich bedeutsame „Unzuverlässigkeit" ist in der Rechtsprechung geklärt, dass diese kein subjektiv vorwerfbares Verhalten voraussetzt, sondern lediglich an *objektive* Tatsachen anknüpft, die hinsichtlich der zukünftigen (ordnungsgemäßen) Tätigkeit des Gewerbetreibenden eine ungünstige Prognose rechtfertigen.[30] Trotz des prognostischen Elements handelt es sich bei der (Un)Zuverlässigkeit um einen gerichtlich umfassend überprüfbaren unbestimmten Rechtsbegriff ohne Beurteilungsspielraum.[31]

19 Übertragen auf den datenschutzrechtlichen Bereich erfasst die Fachkunde dort jedenfalls Kenntnisse des nationalen und europäischen Datenschutzrechts. Die konkreten Fachkenntnisse haben sich an der Sensitivität, Komple-

26 Siehe https://www.katholisches-datenschutzzentrum.de/meldung-bdsb/ (letzter Zugriff: Juni 2019). Die Daten werden unmittelbar in eine zentrale Datenbank eingespeist, welche die spätere Kontaktaufnahme mit den Datenschutzbeauftragten vereinfacht, s. dazu: Diözesandatenschutzbeauftragter für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und Verbandsdatenschutzbeauftragter des Verbandes der Diözesen Deutschlands (Hrsg.), Dritter Jahresbericht für den Zeitraum 1.1.2018 – 31.12.2018, Dortmund 2019, S. 33.

27 Raum in Auernhammer DS-GVO Art. 37 Rn. 73.

28 AA Helfrich in HK-DS-GVO Art. 37 Rn. 113 (mwN), nach dem nach Inkrafttreten der DS-GVO nicht mehr auf die zum nationalen Recht entwickelten Grundsätze zurückgegriffen werden könne.

29 BVerwG NVwZ-RR 2003, 432; Papsthart in Heinrich/ders., Waffenrecht, 9. Aufl. 2010, § 7 Rn. 2; Gade, Waffengesetz, 2. Aufl. 2018, § 7 Rn. 3.

30 Siehe Ennuschat in Tettinger/Wank/Ennuschat GewO § 35 Rn. 27; BVerwG GewArch 1966, 77 (80, 81); BVerwGE 65, 1; zuletzt wieder OVG Münster Beschl. v. 9.4.2019 – 4 B 321/19, 4 E 191/19, juris, Rn. 9.

31 Ennuschat in Tettinger/Wank/Ennuschat GewO § 35 Rn. 27; BVerwGE 28, 202 (209 f.).

xität und dem Umfang der Verarbeitungsvorgänge zu orientieren.[32] Das Tatbestandsmerkmal „zur Erfüllung seiner Aufgaben" (zugleich ein Verweis auf § 38 KDG) spricht für das Erfordernis eines einrichtungs- und tätigkeitsbezogenen Fachwissens. Es macht in der Praxis einen Unterschied, ob es sich um Gesundheits- oder Arbeitnehmerdaten oder um solche von Kindern und Jugendlichen handelt, etwa im Bereich der Jugendhilfe. Das LG Ulm[33] hat in einer älteren Entscheidung über bloße Rechtskenntnisse hinaus ebenfalls gefordert, dass der bDSB über Kenntnisse der betrieblichen Organisation verfügen und „Computerexperte" sein müsse. Von ihm werden zusätzlich didaktische Fähigkeiten, psychologisches Einfühlungsvermögen und Organisationstalent verlangt. Vereinzelte Stimmen fordern auch betriebswirtschaftliche und Management-Kenntnisse.[34] Die vor dem Hintergrund der persönlichen Eignung für die Erfüllung der Aufgaben gem. § 38 KDG zu stellenden Anforderungen an die Fachkunde dürfen aber weder überzogen noch zu gering veranlagt werden. Ein umfassendes „Allround-Wissen", insbesondere ein informationstechnisches oder juristisches Vollstudium, ist nicht notwendig. Demgegenüber dürfte das bloße Kennen und sichere Anwenden von datenschutzrechtlichen Regelungen wohl nicht ausreichen.

Mit – die (Erz-)Diözesen rechtlich nicht bindendem – Beschluss vom 8.2.2018 hat die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland[35] die Mindestanforderungen für die „Fachkunde" näher spezifiziert und Kenntnisse gefordert in den Bereichen „Grundlagen der Arbeit", „Rechtliche Aspekte", „Technische Aspekte" sowie „Organisation der Arbeit" (wird jeweils weiter unterteilt). Für den Nachweis der Fachkunde sei keine Zertifizierung notwendig. Mit Blick auf die zunehmende Komplexität der Arbeit kirchlicher Datenschutzbeauftragter sowie das zu den Anforderungen an die Fachkunde vorliegende disparate Meinungsbild wäre eine einheitliche kirchliche Zertifizierung jedoch sinnvoll. 20

Die Prüfung der **Zuverlässigkeit** ist der Benennung vorgelagert, so dass der bDSB dann „unzuverlässig" im Sinne der Vorschrift ist, wenn sein bisheriges dienstliches Verhalten, insbesondere in datenschutzrelevanter Hinsicht, auf Grundlage einer Prognoseentscheidung des Verantwortlichen nicht den Schluss zulässt, dieser werde die an ihn gem. § 38 KDG gerichteten Aufgaben ordnungsgemäß erfüllen. Zweifel an der Zuverlässigkeit können darüber hinaus auch bestehen, wenn die bisher bzw. auch nach der Benennung noch wahrzunehmenden dienstlichen Verpflichtungen zu einem Interessenkonflikt führen.[36] Diesen Zusammenhang macht § 36 Abs. 7 KDG nochmals gesondert deutlich. 21

32 Gola, Aus den aktuellen Berichten der Aufsichtsbehörden (37): Der DSB nach DS-GVO und neuem nationalem Datenschutzrecht RDV 2018, 257 (258); von Walter, Der Datenschutzbeauftragte, in ders. (Hrsg.), Datenschutz im Betrieb. Die DS-GVO in der Personalarbeit, 2018, S. 41.
33 Zum Folgenden: LG Ulm Beschl. v. 31.10.1990 – CR 1991, 103 (104).
34 Raum in Auernhammer DS-GVO Art. 37 Rn. 77 (mwN).
35 Online abrufbar unter https://www.katholisches-datenschutzzentrum.de/infothek/ (letzter Aufruf: Juni 2020).
36 Kremer in Laue/Kremer Neues DatenschutzR § 6 Rn. 27.

### 8. Benennungshindernis Interessenkonflikt

22 § 36 Abs. 7 KDG versucht der Gefahr konkreter Interessen- und Loyalitätskonflikte zu begegnen, in dem er für den Leiter der Datenverarbeitung sowie den Leiter der kirchlichen Stelle ein gesetzliches Benennungsverbot normiert. Die derzeitige Fassung der Norm als „soll-Vorschrift" irritiert daher, da sie ein Ermessen suggeriert, welches bei den hier geregelten Fällen kaum bestehen kann, möchte man den Regelungshintergrund der §§ 36 ff. KDG nicht ad absurdum führen. Vorliegend geht es – in engem Konnex zu § 37 Abs. 5 KDG – darum, die Benennung solcher Personen zum bDSB zu vermeiden, die aufgrund ihrer bisherigen dienstlichen Stellung ein ausgeprägtes Näheverhältnis zum Verantwortlichen pflegen. Dies gilt insbesondere für die Inhaber kirchlicher Führungspositionen.

23 Auch nach alter Rechtslage (vgl. § 20 Abs. 3 KDO aF iVm § 16 Abs. 2 KDO aF) war die Frage umstritten, ob leitende Mitarbeiter in den Ordinariaten/Generalvikariaten die Position des bDSB ausfüllen können.[37] Verneint wurde die Vereinbarkeit des (nebenberuflichen) Dienstpostens des bDSB für die Leiter der EDV- bzw. Meldewesenabteilungen, da diese sich gleichsam selbst beaufsichtigen und kontrollieren würden. Ebenfalls ausscheiden sollen Leiter und Mitglieder der Personalabteilungen sowie Träger besonderer kirchlicher Ehrentitel: Dort wurde – aufgrund der Nähe zu den diözesanen Verantwortungsträgern – eine Benennung für zumindest heikel angesehen. Wenngleich umstritten (und in Fällen prozessualer Vertretung und Beratung wohl zu Recht kritisiert), wurde die Bestimmung des Diözesanjustitiars zum bDSB doch für zulässig erachtet. Im Bereich des *staatlichen* Datenschutzrechts wurden zusätzlich als ungeeignet angesehen: Geschäftsführer, Vorstand oder Aufsichtsrat, IT-Administrator, Leiter Vertrieb, Geldwäschebeauftragter, Sicherheitsbeauftragter, Betriebsratsvorsitzender.[38]

24 Das bloße Innehaben einer Führungs- bzw. Leitungsposition bewirkt noch keinen Interessenkonflikt. Maßgeblich sind die Nähe der Person zum Verantwortlichen iSd KDG sowie eine Gesamtschau der den zu Benennenden aktuell und zukünftig betreffenden Aufgaben und Pflichten. Personen, die über finanzielle Zuwendungen an die eigene (zukünftige) Dienststelle des bDSB (mit)entscheiden, scheiden ebenso aus wie solche, die strukturell bzw. in der kirchlichen Hierarchie eher „im Lager" des Verantwortlichen stehen. Dies betrifft sicherlich die Leiter der Finanz-, Rechts- und Personalabteilungen, gleichermaßen leitende Angestellte aus dem EDV- und Pressebereich. Bei anderen Führungspositionen besteht ebenso die Gefahr eines Konfliktes mit dem **Überlastungsverbot aus § 36 Abs. 7 S. 2 KDG**, sofern die bisherige Aufgabenbelastung eine ordnungsgemäße Erfüllung der zusätzlichen Aufgaben des bDSB ausschließen würde.

25 Das Überlastungsverbot, abgeleitet aus dem Rechtsgedanken des Art. 38 Abs. 6 DS-GVO, verbietet nicht die Aufgabenwahrnehmung des bDSB „im Nebenamt". Die Aufgabenfülle bzw. ihr Zuschnitt darf nicht zu einem Inter-

37 Dazu: Ausführungen zum Betrieblichen Datenschutzbeauftragten nach § 20 KDO, S. 1 (4 ff.).

38 Vgl. Kremer in Laue/Kremer Neues DatenschutzR § 6 Rn. 27. Nach BAG RDV 2012, 237, besteht jedoch keine generelle Unvereinbarkeit zwischen dem Amt des dDSB und einer Betriebsratsmitgliedschaft. Entsprechendes gilt für die Mitarbeitervertretungen in kirchlichen Einrichtungen.

tigt.[119] Geklagt haben fünf spanische Supermarktkassiererinnen gegen eine verdeckte Videoüberwachung ihres Arbeitgebers, der aufgrund Diebstahlverdachts zehn Tage lang im Verkaufsraum verdeckt eine Videokamera laufen ließ. Der EGMR hob eine anderslautende Entscheidung der Kleinen Kammer des EGMR vom 9. Januar 2018 wieder auf. Zwar müssten Beschäftigte grundsätzlich über die geplante Überwachung informiert werden, um ihre Persönlichkeitsrechte zu schützen. Im vorliegenden Fall habe der Arbeitgeber aber kaum eine andere Möglichkeit besessen, den Diebstahl aufzuklären. Er habe die Videoüberwachung sowohl räumlich – nur der Kassenbereich, nicht der ganze Supermarkt – als auch zeitlich auf das erforderliche Maß beschränkt und umgehend nach Aufklärung des Diebstahlverdachts nach zehn Tagen beendet. Ein milderes – effektives – Mittel hätte es nicht gegeben. Darüber hinaus seien die Auswirkungen auf die Privatsphäre der Beschäftigten in einem ohnehin öffentlichen Bereich wie den Supermarktkassen überschaubar gewesen. Der EGMR hebt allerdings ausdrücklich hervor, dass ohne die Kenntlichmachung und Vorabinformation der Überwachung die anderen Kriterien für die Rechtmäßigkeit einer verdeckten Videoüberwachung umso strenger geprüft werden müssten.

#### d) Heimliche Videoüberwachung in nicht öffentlich zugänglichen Räumen

Die verdeckte Videoüberwachung nicht öffentlich zugänglicher Arbeitsplätze richtet sich, soweit Beschäftigte betroffen sind, nach § 53 KDG. Ebenso wie bei der verdeckten Überwachung öffentlich zugänglicher Räume stellt sich auch hier die Frage nach der generellen Zulässigkeit eines solchen Vorgehens. Von der arbeitsgerichtlichen Judikatur wird die Zulässigkeit einer solchen Maßnahme grundsätzlich bejaht, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Vertragsverletzung zulasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist.[120] 50

Die **Mitarbeitervertretung** hat bei Einführung und Ausgestaltung einer Videoüberwachung nach § 36 Abs. 1 Nr. 9 MAVO mitzubestimmen. 51

## § 53 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

**(1) Personenbezogene Daten eines Beschäftigten einschließlich der Daten über die Religionszugehörigkeit, die religiöse Überzeugung und die Erfüllung von Loyalitätsobliegenheiten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäf-**

119 EGMR 17.10.2019 – 1874/13, NJW 2020, 141 f.; vgl. hierzu auch Körner NZA 2020, 25 (27); Hembach NJW 2020, 128. – In anderen Fällen hat der EGMR die Videoüberwachung teilweise gebilligt, wie etwa im Fall „Köpke" (EGMR 5.10.2010 – 420/07, EuGRZ 2011, 471) und teilweise für unzulässig erklärt, wie etwa im Fall „Barbulescu" (EGMR 5.9.2017 – 61496/08, NZA 2017, 1443).

120 BAG 28.10.2016 – 2 AZR 395/15, Rn. 22; BAG 29.6.2017 – 2 AZR 597/16, Rn. 32.

**tigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.**

**(2) Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind oder eine Rechtsvorschrift dies vorsieht.**

**(3) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten verarbeitet werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet oder für die Verarbeitung in einer solchen Datei erhoben werden.**

**(4) Die Beteiligungsrechte nach der jeweils geltenden Mitarbeitervertretungsordnung bleiben unberührt.**

## A. Gesamtverständnis und Zweck der Norm

Die zentrale Anknüpfungsnorm für den Beschäftigtendatenschutz auf europäischer Ebene ist Art. 88 DS-GVO. Sie enthält eine Öffnungsklausel zugunsten der Mitgliedstaaten für die Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen. Danach können die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Datenschutzbestimmungen hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungskontext vorsehen. Der **Bundesgesetzgeber** hat von dieser Gestaltungsmöglichkeit Gebrauch gemacht, indem er mit § 26 BDSG eine eigene Rechtsgrundlage für Datenverarbeitungen im Beschäftigungskontext geschaffen hat. § 26 BDSG ersetzt die bisherige Bestimmung des § 32 BDSG aF Ziel der Novelle war es, die Vorläuferbestimmung inhaltlich fortzuführen und an die Terminologie der DS-GVO anzupassen, nicht aber grundlegend zu ändern.[1] § 26 BDSG regelt das Beschäftigtendatenschutzrecht für die Beschäftigten in der **Privatwirtschaft** und in den **Bundesbehörden**; der Beschäftigtendatenschutz der **Landes- und Kommunalbediensteten** ist in den Datenschutzgesetzen der 16 Bundesländer niedergelegt, die ebenfalls von der Ermächtigungsnorm des Art. 88 DS-GVO Gebrauch gemacht haben.[2] 1

Im Bereich der **Kirchen und Religionsgemeinschaften** findet weder die DS-GVO noch das profane deutsche Datenschutzrecht Anwendung. Kirchen und Religionsgemeinschaften dürfen gemäß Art. 91 DS-GVO ihre eigenen Datenschutzregelungen – auch im Beschäftigungskontext[3] – anwenden, sofern sie mit den Standards der DS-GVO in Einklang stehen. Das In-Einklang-Bringen fordert keine 1:1-Umsetzung oder völlige Deckungsgleichheit;[4] dem kirchlichen Gesetzgeber muss ein gewisser Gestaltungsspielraum verbleiben.[5] Die kircheneigenen Regelwerke zum Datenschutz sind als umfassende und kohärente Kodifikationen konzipiert, die den Anspruch erheben, sich auf alle Bereiche des Datenschutzrechts zu erstrecken, damit auch auf den Beschäftigtendatenschutz im kirchlichen Dienst.[6] Um etwaige Schutzlücken im Detail zu schließen, können materielle Regelungen der DS-GVO bzw. des BDSG sowie die hierzu ergangene Rechtsprechung im Einzelfall entsprechend herangezogen werden.[7] 2

Damit das kirchliche Datenschutzrecht in seinem Schutzniveau nicht hinter den europäischen Vorgaben zurückbleibt, sind die bislang bestehenden kirchlichen Datenschutzbestimmungen an die DS-GVO angepasst worden. Zu diesem Zweck haben die **evangelische** und **katholische Kirche** in Deutschland auch ihre **Regelungen zum kirchlichen Beschäftigtendatenschutzrecht** neu gefasst. Im EKD-Datenschutzgesetz ist die Verarbeitung personenbezogener Daten in Dienst- und Arbeitsverhältnissen hauptsächlich in **§ 49 DSG-EKD** geregelt. Für die Beschäftigten in den Einrichtungen der katholischen Kirche ist der Beschäftigtendatenschutz im Wesentlichen in **§ 53 KDG** niedergelegt. 3

1 BT-Drs. 18/11322*5*, S. 97.
2 Exemplarisch: § 18 DSG-NRW; § 23 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG).
3 Grages in Plath DS-GVO Art. 91 Rn. 4.
4 Losem KuR 2013, 231 (242).
5 Hense in HK-DS-GVO Art. 91 Rn. 20 mwN; Thüsing/Rombey in Schwartmann/Jaspers/Thüsing/Kugelmann Art. 91 DS-GVO Rn. 13 mwN.
6 Hense in HK-DS-GVO Art. 91 Rn. 18.
7 Grages in Plath DS-GVO Art. 91 Rn. 2.

Die Vorschrift ist weitgehend inhaltsgleich mit dem früheren § 10 a KDO. Die novellierte Bestimmung verwendet allerdings den Begriff der „Verarbeitung", womit nunmehr jede Form der Behandlung von personenbezogenen Daten erfasst wird, vgl. § 4 Nr. 3 KDG. Darüber hinaus verdienen im kirchlich-katholischen Beschäftigungskontext § 6 Abs. 1 a), b) und d) KDG, § 8 KDG sowie § 11 Abs. 2 a), b) und h) KDG besondere Beachtung. In materieller Hinsicht orientiert sich die Bestimmung des § 53 KDG an § 26 BDSG nF Die lediglich geringfügigen Modifikationen im Vergleich zum früheren Recht verdeutlichen, dass es dem weltlichen wie dem kirchlichen Gesetzgeber darum ging, die bisherige Rechtslage im Wesentlichen zu perpetuieren. Die Erlaubnistatbestände der bisherigen Regelung und die dazu ergangene Judikatur erfuhren durch die letzte Novelle gewissermaßen eine legislative Bestätigung.

## B. Verhältnis zur DS-GVO bzw. zum BDSG und Grundlagen

### I. Öffnungsklausel für kirchenspezifische Regelungen im Beschäftigungsverhältnis

4 Mit der Schaffung des § 53 KDG hat der kirchliche Gesetzgeber im Bereich der katholischen Kirche in Deutschland von der Regelungsbefugnis des Art. 88 DS-GVO Gebrauch gemacht, der über die Brückennorm des Art. 91 DS-GVO mittelbar auch eine **Öffnungsklausel für kirchenspezifische Regelungen** enthält. Die den Religionsgemeinschaften eröffnete Möglichkeit zur eigenen Rechtsetzung entbindet sie jedoch nicht davon, die Vorgaben des europäischen Datenschutzrechtes zu beachten. Nach ganz überwiegender Auffassung im Schrifttum stellt die DS-GVO im Verhältnis zum mitgliedstaatlichen[8] bzw. kirchlichen[9] Beschäftigtendatenschutz einen **Mindeststandard** dar, den weder der mitgliedstaatlich-weltliche noch der kirchliche Gesetzgeber unterschreiten dürfen. Allerdings steht es dem kirchlichen Gesetzgeber frei, für seine Beschäftigten günstigere kirchliche Regelungen, in denen ein **höheres Datenschutzniveau** gilt, zu erlassen.[10]

### II. Kirchliche Rechtsvorschriften

5 Kirchen und Religionsgemeinschaften können gemäß Art. 88 DS-GVO iVm Art. 91 DS-GVO durch „**Rechtsvorschriften**" oder durch „**Kollektivvereinbarungen**" spezifischere Datenschutzvorschriften hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungskontext vorsehen. Der Begriff der „Rechtsvorschriften" umfasst **gesetzliche** und **untergesetzliche** Regelungen. Zu ihnen zählen in der kirchlichen Rechtssphäre insbesondere **allgemeine** und **partikulare** Kirchengesetze (vgl. cc. 7, 8 CIC). So ist zB das KDG in

8 Kort DB 2016, 711 (714): „Eine Absenkung des Niveaus der DS-GVO ist somit im Ergebnis nicht möglich"; Gola/Pötters/Thüsing RDV 2016, 58 (59); Tiedemann in HK-DS-GVO Art. 88 Rn. 3; Stahmer/Kuhnke in Plath DS-GVO Art. 88 Rn. 6.

9 Hense in HK-DS-GVO Art. 91 Rn. 21 mwN.

10 Teile der Literatur postulieren ein Gebot der Vollharmonisierung, aus dem sie ableiten, dass eine Abweichung „nach oben" unzulässig sei. So folgert zB Maschmann aus dem EuGH-Urteil vom 24.11.2011 in Sachen ASNEF, dass der nationale Gesetzgeber – und konsequent dann auch der kirchliche Gesetzgeber sowie die Betriebspartner in einer Kollektivvereinbarung – das Datenschutzniveau nicht zugunsten des Betroffenen anheben dürfen, vgl. Maschmann in Kühling/Buchner DS-GVO Art. 88 Rn. 32 ff.

der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20.11.2017 als **partikulares Kirchengesetz** nahezu wortlautidentisch in allen 27 (Erz-)Diözesen in Kraft gesetzt worden.

Auch **allgemeine Ausführungsdekrete** (c. 29 CIC), „durch welche die Art und Weise der Gesetzesanwendung genauer bestimmt oder die Befolgung der Gesetze eingeschärft wird" (c. 31 § 1 CIC) und die für ihre kirchenrechtliche Wirksamkeit promulgiert werden müssen (c. 31 § 2 CIC), sind als Rechtsvorschriften im Sinne des Art. 88 DS-GVO anzuerkennen, wenn sie klar und präzise und in ihrer Anwendung für den Rechtsunterworfenen vorhersehbar sind. Sie entfalten Rechtsverbindlichkeit nur innerhalb der Grenzen des jeweiligen Bezugsgesetzes; der Normadressatenkreis entspricht jenem des Bezugsgesetzes.[11] Das als „Durchführungsverordnung zum KDG" titulierte Regelwerk ist als ein Ausführungsdekret im Sinne des c. 29 CIC zu qualifizieren; er wurde in den diözesanen Amtsblättern promulgiert. 6

Kanonistische **Instruktionen** (c. 34 CIC) ähneln den allgemeinen Ausführungsdekreten, auch sie erklären die kirchengesetzlichen Bestimmungen und enthalten Anweisungen für ihre Ausführung. Da sie aber keine Außenwirksamkeit entfalten, ist eine förmliche Promulgation entbehrlich.[12] Instruktionen sind daher lediglich intern wirkendes kirchliches **Binnenrecht**, das keine Bindungswirkung nach außen entfaltet, insbesondere nicht gegenüber kirchlichen Beschäftigten. Daher werden sie vom Begriff „Rechtsvorschriften" nicht erfasst, weil ihnen sowohl nach weltlichem als auch nach kirchlichem Recht die normative Wirkung gegenüber den Rechtsunterworfenen fehlt. 7

Ob **höchstrichterliche Rechtsgrundsätze** bzw. eine **ständige Rechtsprechung** unter den Begriff „Rechtsvorschriften" subsumiert werden können, wird im Schrifttum zum weltlichen Beschäftigtendatenschutzrecht kontrovers diskutiert.[13] Zuzustimmen ist der Auffassung, wonach zumindest die **Klärung** und **Konkretisierung** des beschäftigtendatenschutzrechtlichen Normbestandes durch die höchstrichterliche Judikatur einen Bestandteil der Rechtsvorschriften zum Beschäftigtendatenschutz bildet, zumal der Arbeitnehmerdatenschutz in Deutschland seit jeher vorwiegend richterrechtlich geprägt ist und der Gesetzgeber sich bislang überwiegend darauf beschränkt hat, die von der Judikatur erarbeiteten Grundsätze zu kodifizieren. Daraus folgt: So wie im weltlichen Bereich die Auslegung des BAG zu § 32 BDSG aF bzw. zu § 26 BDSG nF eine gesetzesgleiche Wirkung entfalten kann, so gilt dies auch in der kirchlichen Rechtssphäre bzgl. der Rechtsprechung der kirchlichen Revisionsgerichte, namentlich des Kirchlichen Arbeitsgerichtshofs (KAGH) und des Datenschutzgerichts der Deutschen Bischofskonferenz (DSG-DBK), zur Auslegung des KDG. 8

### III. Kirchliche Kollektivvereinbarungen

Art. 88 DS-GVO ermöglicht auch eine Regelung des Datenschutzrechts auf der Grundlage von **Kollektivvereinbarungen**, wobei die Verhandlungspartner Art. 88 Abs. 2 DS-GVO zu beachten haben. Damit können **Tarifverträge**, **Betriebs-** oder **Dienstvereinbarungen** eine eigene **Rechtsgrundlage** für die Rege- 9

11 HdbKathKR-Kalb, 3. Aufl., S. 167.
12 HdbKathKR-Kalb, 3. Aufl., S. 168.
13 Ablehnend: HK-Thüsing/Traut in Schwartmann/Jaspers/Thüsing/Kugelmann DS-GVO Art. 88 Rn. 38. Zustimmend: Tiedemann in HK-DS-GVO Art. 88 Rn. 8.

lungen zum Beschäftigtendatenschutz bilden. Anders als der weltliche Gesetzgeber, der dieses – auch vor dem Inkrafttreten der DS-GVO schon anerkannte – Regelungsinstrument in § 26 Abs. 4 BDSG explizit aufgenommen hat, verzichtet der kirchliche Gesetzgeber im Rahmen des § 53 KDG auf eine ausdrückliche Erwähnung der **kirchlichen Kollektivvereinbarungen**. Dessen ungeachtet besteht kein Zweifel daran, dass auch im kirchlichen Beschäftigungskontext **mitarbeitervertretungsrechtliche Dienstvereinbarungen** (vgl. § 38 MAVO) und **kirchliche Arbeitsvertragsregelungen des Dritten Weges** (vgl. Art. 7 Abs. 1 S. 2 GrO, zB AVR-Caritas) eine datenschutzrechtliche Erlaubnisgrundlage bilden können. Die Schaffung kirchlicher Kollektivvereinbarungen obliegt einerseits den Repräsentationsorganen im kirchlichen Betriebsverfassungsrecht (MAVO), insbesondere Mitarbeitervertretung (MAV), Gesamtmitarbeitervertretung (GMAV) und erweiterte Gesamtmitarbeitervertretung (eGMAV) und den Dienstgebern, andererseits den Verhandlungspartnern in den paritätisch zusammengesetzten arbeitsrechtlichen Kommissionen des Dritten Weges. Nach kirchlichem Selbstverständnis kommt den kirchenarbeitsrechtlichen Kollektivvereinbarungen **normative Wirkung** zumindest gegenüber den Verantwortlichen zu (vgl. § 38 Abs. 3 a MAVO; § 3 Abs. 1 S. 2 Rahmen-KODA-Ordnung). In datenschutzrechtlicher Hinsicht stellen die kirchlichen Kollektivvereinbarungen **spezifisch kirchenarbeitsrechtliche Verpflichtungen im Sinne des § 6 Abs. 1 d) KDG** dar, denen der Verantwortliche unterliegt. Auch ohne ausdrückliche Nennung in § 53 KDG kommen sie daher als Rechtfertigungstatbestände für die rechtmäßige Verarbeitung personenbezogener Daten im Rahmen des § 6 KDG zur Anwendung. Dienstvereinbarungen nach der MAVO und kirchliche Arbeitsvertragsregelungen können auf diese Weise mittelbar Bestimmungen zur Verarbeitung personenbezogener Daten enthalten.

### IV. Verarbeitung besonders sensibler Daten im Beschäftigungskontext

10 Für die **Verarbeitung besonderer Kategorien personenbezogener Daten** (§ 4 Nr. 2 KDG) wiederholt § 11 Abs. 2 b) KDG die Ermächtigung, die sich bereits in Art. 88 Abs. 1 DS-GVO findet. Nach dieser Bestimmung, die im Wesentlichen inhaltsgleich mit § 26 Abs. 3 u. 4 BDSG ist, ist die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist, soweit kirchliches oder staatliches Recht oder eine Dienstvereinbarung nach der Mitarbeitervertretungsordnung Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen. Die Bestimmung bringt zum Ausdruck, dass die Kollektivvertragsparteien an Grundrechte gebunden sind, insbesondere an das informationelle Selbstbestimmungsrecht. Sie dürfen nicht zulasten der Beschäftigten von der DS-GVO abweichen. Die allgemeinen datenschutzrechtlichen Grundsätze, wie sie in Art. 5 DS-GVO bzw. § 7 KDG festgehalten sind, sind für sie verbindlich.

### V. Einwilligung im kirchlichen Beschäftigtendatenschutzrecht

11 § 26 Abs. 2 BDSG enthält eine Klarstellung, wonach **Einwilligungen** auch im Rahmen von Arbeitsverhältnissen **grundsätzlich zulässig** sind, wenn bestimmte Voraussetzungen erfüllt sind. Europarechtlich ergibt sich die Mög-

lichkeit der Einwilligung im Arbeitsverhältnis aus Erwägungsgrund 155 iVm Art. 7 DS-GVO. Soll die Verarbeitung von Beschäftigtendaten auf die Einwilligung der betroffenen Person gestützt werden, sind strenge Wirksamkeitsbedingungen zu beachten. Bei der rechtlichen Beurteilung der Einwilligung spielt insbesondere die Frage, ob sie **freiwillig** erteilt wurde, eine entscheidende Rolle.[14]

12 Für die Freiwilligkeit sind in erster Linie **die in jedem Beschäftigungsverhältnis bestehende Abhängigkeit** des Beschäftigten sowie die **Umstände, unter denen die Einwilligung erteilt worden ist**, zu berücksichtigen. Ausweislich der amtlichen Gesetzesbegründung ist neben der Art des verarbeiteten Datums und der Eingriffstiefe auch der **Zeitpunkt der Einwilligungserteilung** maßgebend. Vor Abschluss eines (Arbeits-)Vertrages werden Beschäftigte regelmäßig einer größeren Drucksituation ausgesetzt sein, eine Einwilligung in eine Datenverarbeitung zu erteilen.[15] Freiwilligkeit kann nach § 26 Abs. 2 S. 2 BDSG insbesondere vorliegen, wenn für die beschäftigte Person **ein rechtlicher oder wirtschaftlicher Vorteil** erreicht wird oder Arbeitgeber und Beschäftigter **gleichgelagerte Interessen** verfolgen. Die Gewährung eines Vorteils liegt beispielsweise in der Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder in der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen.[16] Eine Verfolgung gleichgerichteter Interessen ist nach der Gesetzesbegründung zu § 26 BDSG etwa anzunehmen, wenn der Beschäftigte der Aufnahme seines Namens und seines Geburtsdatums in eine Geburtstagsliste oder der Veröffentlichung seines Fotos im Intranet zustimmt.[17]

13 Als **formelle Voraussetzung einer Einwilligung** ordnet § 26 Abs. 2 S. 3 BDSG grundsätzlich die **Schriftform** an, um die informationelle Selbstbestimmung der betroffenen Beschäftigten abzusichern. Damit wird die Nachweispflicht des Arbeitgebers im Sinne von Art. 7 Abs. 1 DS-GVO konkretisiert. Hinzu kommt die Pflicht des Arbeitgebers zur **Aufklärung** in Textform über den Zweck der Datenverarbeitung und den jederzeit möglichen Widerruf durch den Beschäftigten sowie dessen Folgen nach Art. 7 Abs. 3 DS-GVO.

14 Diese in § 26 BDSG formulierten **Vorgaben für die Einwilligung gelten im Grunde auch im Rahmen des kirchlichen Beschäftigtendatenschutzes**. Regelungstechnisch finden sich die Anforderungen an eine wirksame Einwilligung jedoch nicht in § 53 KDG, sondern in § 8 KDG. Der kirchliche Gesetzgeber hat die Voraussetzungen einer wirksamen Einwilligung nicht bereichsspezifisch definiert, sondern vor die Klammer gezogen, um ein und dieselbe Vorschrift nicht an mehreren Stellen des KDG wiederholen zu müssen. Wie im weltlichen Recht so gilt auch im kirchlichen Bereich der Grundsatz, dass die

14 „Das Besondere" des Beschäftigtendatenschutzes gegenüber dem allgemeinen Datenschutz erblickt Joussen zu Recht darin, „dass die Möglichkeit des eigenen Tätigwerdens im Hinblick auf den Umgang mit den Daten geringer ist. Während im Privatleben jedermann weitgehend selbst darüber entscheiden kann, welche Medien er nutzen möchte und welche Daten er zu welchen Zwecken auf diesem Wege weitergeben will, ist ein derartiger Selbstschutz im Arbeitsleben weitgehend ausgeschlossen. Hier treffen insoweit Datenschutz und Direktionsrecht aufeinander", so Joussen NZA Beilage 1/2011, 35 (37).

15 BT-Drs. 18/113225, 97.

16 BT-Drs. 18/113225, 97.

17 BT-Drs. 18/113225, 97.

Einwilligung nur wirksam ist, wenn sie **auf einer freien Entscheidung** der betroffenen Person beruht, § 8 Abs. 1 S. 2 KDG. An der erforderlichen Freiwilligkeit fehlt es insbesondere dann, wenn dem Betroffenen die Einwilligung unter Ausnutzung einer wirtschaftlichen Machtposition abgenötigt wurde oder der Betroffene einwilligen „muss", um eine begehrte Leistung, wie etwa einen Arbeitsplatz zu erhalten bzw. zu behalten. Im kirchlichen Datenschutzrecht setzt eine wirksame Einwilligung nicht nur im Beschäftigungskontext, sondern ganz allgemein die **Schriftform** voraus, § 8 Abs. 2 S. 1 KDG. Eine Abweichung vom Schriftformerfordernis kommt nur ausnahmsweise in Betracht, wenn „wegen besonderer Umstände eine andere Form angemessen ist". Eine andere Form in diesem Sinne kann grundsätzlich nur die Erklärung in Textform (E-Mail, Fax usw) oder eine ausdrückliche nachweisbare mündliche Einwilligung sein. Eine stillschweigende Hinnahme durch den Beschäftigten reicht dagegen nicht aus. Daraus folgt, dass nur eine aktive und unmissverständliche Willensbetätigung durch den Einwilligenden als wirksame Einwilligung gelten kann. Eine wirksame Einwilligung liegt nur vor, wenn sie erteilt wird, **bevor** die Datenverarbeitung erfolgt. Ein nachträgliches Einverständnis reicht demnach nicht aus.

15 Das Schriftformerfordernis wird schon aufgrund der erforderlichen **Nachweisbarkeit der Einwilligung** regelmäßig unerlässlich sein, vgl. § 8 Abs. 5 KDG. Die Folgen einer Einwilligung müssen für die betroffene Person transparent sein. Das Ersuchen um eine schriftliche Einwilligung muss „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erfolgen; es muss zudem „von anderen Sachverhalten" klar zu unterscheiden sein, § 8 Abs. 2 S. 2 KDG. Dies kann durch besondere Hervorhebung (zB Fettdruck) erfolgen. Ist die Unterscheidung nicht deutlich genug, ist die Einwilligung unbeachtlich. In der Praxis empfiehlt es sich, eine Einwilligung **durch gesondertes Schreiben** einzuholen und nicht nur einen entsprechenden Passus, zB im Arbeitsvertrag oder im Einladungsschreiben zum Vorstellungsgespräch, vorzusehen. In dem gesonderten Schreiben sollten **die jeweiligen Daten** und **ihr Verwendungszweck** ausdrücklich benannt werden. Bei besonderen Kategorien personenbezogener Daten (§ 4 Nr. 2 KDG) muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen, § 8 Abs. 4 KDG.

### VI. Erforderlichkeit und Verhältnismäßigkeit der Datenverarbeitung

16 Analog zum weltlichen Recht verlangt § 53 Abs. 1 KDG, dass die Verarbeitung für die genannten Zwecke **erforderlich** ist. Im Rahmen der Erforderlichkeitsprüfung sind die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen. Darin manifestiert sich der vom BAG in ständiger Rechtsprechung entwickelte Grundsatz, wonach die Erforderlichkeit der Datenverarbeitung anhand einer am **Verhältnismäßigkeitsprinzip** ausgerichteten **Interessenabwägung** vorzunehmen ist.[18] Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beiden Interessen möglichst weitgehend Rechnung trägt.[19] Die Rechtspre-

18 BAG 27.7.2017 – 2 AZR 681/16, Rn. 30; BAG 29.6.2017 – 2 AZR 597/16, Rn. 32; BAG 17.11.2016 – 2 AZR 730/15, Rn. 30.
19 BT-Drs. 18/11325, 97.

chung verlangt, dass der Eingriff **geeignet, erforderlich** und unter Berücksichtigung der gewährleisteten Freiheitsrechte **angemessen** ist, um den erstrebten Zweck zu erreichen. Es dürfen keine anderen, zur Zielerreichung gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkenden Mittel zur Verfügung stehen. Die Verhältnismäßigkeit im engeren Sinne (Angemessenheit) ist gewahrt, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Die Datenverarbeitung darf keine übermäßige Belastung für den Arbeitnehmer darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen.[20]

## C. Kommentierung

### I. Anwendungsbereich

#### 1. Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich des § 53 KDG umfasst alle „**Beschäftigten**" im kirchlichen Dienst. Die katholische Kirche in Deutschland mit ihrer Caritas hat bundesweit ca. 800.000 hauptamtliche Beschäftigte. Davon sind etwa 660.000 hauptberufliche Mitarbeiter in 24.780 Einrichtungen der Caritas tätig.[21] 17

Das Beschäftigtendatenschutzrecht der katholischen Kirche findet nur dort Anwendung, wo **kirchliches Arbeitsrecht** gilt. Das ist nur bei den Anstellungsträgern der Fall, die unmittelbar der bischöflichen Gesetzgebungsgewalt im Sinne des Art. 2 Abs. 1 GrO unterliegen oder die durch die Übernahme der „Grundordnung des kirchlichen Dienstes im Rahmen kirchlicher Arbeitsverhältnisse" in ihr Statut gemäß Art. 2 Abs. 2 GrO sich für das kirchliche Arbeitsrechtsregime entschieden haben.[22] Im Umkehrschluss bedeutet das: Wer nicht der kirchlichen Arbeitsrechtsordnung unterliegt, kann sich auch nicht auf kirchliches Beschäftigtendatenschutzrecht berufen. Es gilt insoweit weltliches Beschäftigtendatenschutzrecht. 18

Der Beschäftigtenbegriff wird eigenständig in § 4 Nr. 24 KDG definiert. 19

Zu den dort aufgezählten Personengruppen zählen ua **Kleriker** und **Kandidaten für das Weiheamt**, § 4 Nr. 24 a) KDG. Kleriker stehen in einem besonderen kirchenrechtlich geprägten Dienstverhältnis zu ihrem Bischof (c. 275 § 2 CIC). Der Weltgeistliche gehört in der Regel einer Diözese an, der Ordensgeistliche einer Ordensgemeinschaft. 20

Auch für **Ordensangehörige** gilt das kirchliche Beschäftigtendatenschutzrecht, soweit sie auf einer Planstelle in einer Einrichtung der eigenen Ordensgemeinschaft oder aufgrund eines Gestellungsvertrages tätig sind, § 4 Nr. 24 b) KDG. 21

Darüber hinaus findet kirchliches Beschäftigtendatenschutzrecht Anwendung auf alle **Beschäftigten im kirchlichen Dienst**, die aufgrund eines zivilrechtlichen Arbeits- oder eines kirchlichen Beamtenverhältnisses beschäftigt sind, § 4 Nr. 24 c). Dieser Personenkreis macht mit Abstand den größten Anteil an der Gesamtzahl der Beschäftigten aus. Zu dieser Gruppe gehören alle Dienst- 22

20 BAG 27.7.2017 – 2 AZR 681/16, Rn. 30.
21 Katholische Kirche in Deutschland. Zahlen und Fakten, 2018/2019. Arbeitshilfe 306, hrsg. Sekretariat der Deutschen Bischofskonferenz, S. 37.
22 Ausführlich hierzu Fuhrmann ZAT 2013, 9 ff.

nehmer in der Kirche, die durch einen Arbeitsvertrag zur Leistung weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit verpflichtet sind (§ 611 a Abs. 1 S. 1 BGB). Kirchliche Beamte werden in ein kirchliches Beamtenverhältnis aufgenommen; sie erhalten keinen Arbeitsvertrag, sondern eine Ernennungsurkunde.[23]

23 Einbezogen sind ferner die **zu ihrer Berufsbildung tätigen Personen** mit Ausnahme der Postulanten und Novizen, § 4 Nr. 24 d) KDG. Hierzu gehören nicht nur Auszubildende, sondern nach § 1 Abs. 1 BBiG auch Personen in beruflicher Fortbildung, beruflicher Umschulung und solche in Berufsausbildungsvorbereitung.

24 Außerdem fallen **Teilnehmende an Leistungen zur Teilhabe am Arbeitsleben** sowie an **Abklärungen der beruflichen Eignung** oder **Arbeitserprobung** (Rehabilitanden) in den Anwendungsbereich der Norm, § 4 Nr. 24 e) KDG. Dazu zählen insbesondere sog. Ein-Euro-Jobber nach § 16 d SGB II, Personen in Arbeitstherapie nach §§ 27 S. 2 Nr. 6, 42 SGB V sowie solche Personen, die nach längerer Krankheit gemäß § 74 SGB V ein sog. „Wiedereingliederungsverhältnis" begründen, das nach der Rechtsprechung eine Rechtsbeziehung sui generis darstellt.[24]

25 Ebenfalls einbezogen sind Personen, die in anerkannten **Werkstätten für Menschen mit Behinderungen** (**Werkstattbeschäftigte**) tätig sind, § 4 Nr. 24 f.) KDG, vgl. hierzu §§ 219 ff. SGB IX.

26 Außerdem unterfallen dem § 53 KDG auch die Personen, die nach dem **Bundesfreiwilligengesetz oder in vergleichbaren Diensten** (zum Beispiel freiwilliges ökologisches oder soziales Jahr) tätig sind, sowie **Praktikanten**, § 4 Nr. 24 g) KDG. Praktikant ist gemäß § 22 Abs. 1 S. 3 MiLoG unabhängig von der Bezeichnung des Rechtsverhältnisses, wer sich nach der tatsächlichen Ausgestaltung und Durchführung des Vertragsverhältnisses für eine begrenzte Dauer zum Erwerb praktischer Kenntnisse und Erfahrungen einer bestimmten betrieblichen Tätigkeit zur Vorbereitung auf eine berufliche Tätigkeit unterzieht, ohne dass es sich um eine Berufsausbildung im Sinne des Berufsausbildungsgesetzes oder um eine damit vergleichbare praktische Ausbildung handelt.

27 Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als **arbeitnehmerähnliche Personen** einzuordnen sind, unterfallen auch dem kirchlichen Beschäftigtendatenschutz, § 4 Nr. 24 h) KDG.

28 § 4 Nr. 24 i) KDG stellt zudem klar, dass auch **Stellenbewerber** und **ausgeschiedene Beschäftigte** in den Anwendungsbereich der Norm einbezogen sind.

29 Die **Aufzählung** in § 4 Nr. 24 KDG ist **nicht abschließend** („insbesondere"). Dem kirchlichen Beschäftigtendatenschutzrecht unterfallen auch **sonstige Beschäftigte**, etwa Werkstudenten und Schüler, wenn sie während ihrer Studienzeit oder in den Schulferien eine Tätigkeit in einer kirchlichen Einrichtung gegen Entgelt ausüben. Sie gelten in diesen Fällen nicht als Auszubildende, sondern als **Aushilfskräfte**.

23 Zum Kirchenbeamtenrecht in der katholischen Kirche vgl. Ling ZBR 2006, 238 ff.; Schlief KuR 1999, 97 ff.; Sydow KuR 2009, 229 ff.

24 BAG 29.1.1992 – 5 AZR 37/91.

Einbezogen sind auch Beschäftigte, die **aufgrund von Gestellungsverträgen** beschäftigt werden, oder **Leiharbeitnehmer** (§ 1 Abs. 1 S. 1 AÜG), die in kirchlichen Einrichtungen eingesetzt werden. 30

## 2. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich der Norm wird durch die Verarbeitung von personenbezogenen Daten eines Beschäftigten **für Zwecke des Beschäftigungsverhältnisses** bestimmt. Dadurch werden alle Phasen eines Beschäftigungsverhältnisses erfasst. Die Bestimmung regelt also, zu welchen Zwecken und unter welchen Voraussetzungen personenbezogene Daten **vor**, **im** und **nach** Beendigung des Beschäftigungsverhältnisses verarbeitet werden dürfen. Damit unterfällt eine Vielzahl von Regelungsbereichen dem Beschäftigtendatenschutzrecht. In der **Anbahnungsphase** eines Beschäftigungsverhältnisses geht es zum Beispiel um die zulässige inhaltliche Ausgestaltung von Personalfragebögen unter besonderer Beachtung des Grundsatzes der Datenvermeidung (§ 7 Abs. 1 c) KDG), um den Problemkreis der zulässigen bzw. unzulässigen Fragen im Bewerbungsgespräch, um die Frage, ob die Datenerhebung bei Dritten, beispielsweise beim früheren Arbeitgeber, zulässig ist oder um die Frage, ob und wenn ja, unter welchen Voraussetzungen ärztliche Einstellungsuntersuchungen und psychologische Tests erlaubt sind. Im **laufenden Beschäftigungsverhältnis** geht es insbesondere darum zu klären, welche personenbezogenen Daten für die Erfüllung des Arbeitsvertrages, für die Planung, Organisation und Durchführung der Arbeit benötigt und verarbeitet werden dürfen. Datenschutzrechtlich klärungsbedürftig ist auch die Frage, welche personenbezogenen Daten etwa zu Gesundheit und Sicherheit am Arbeitsplatz, zum Schutz des Eigentums des Arbeitgebers oder der Kunden, zur Qualitätskontrolle, Effizienzsteigerung oder Prozessoptimierung verarbeitet werden dürfen. Des Weiteren erstreckt sich das kirchliche Beschäftigtendatenschutzrecht auch auf die Beteiligungsrechte der Interessenvertretung, auf die Maßnahmen der Corporate-Compliance und auf das Betriebsrentenrecht. **Nach Beendigung des Beschäftigungsverhältnisses** steht in erster Linie die Frage im Mittelpunkt, wie mit den personenbezogenen Daten der ausgeschiedenen Beschäftigten zu verfahren ist, insbesondere, wie lange diese Daten aufzubewahren bzw. wann sie spätestens zu löschen sind. 31

**§ 53 Abs. 3 KDG** erweitert den Anwendungsbereich des Beschäftigtendatenschutzes ausdrücklich um die **nicht automatisierte Verarbeitung** personenbezogener Daten. Die Bestimmung entspricht inhaltlich § 26 Abs. 7 BDSG. Das Dateierfordernis des § 2 Abs. 1 KDG wird damit aufgehoben. Das Beschäftigtendatenschutzrecht gilt damit auch für die Verarbeitung personenbezogener Beschäftigtendaten, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Durch diese Erweiterung des Anwendungsbereichs erfasst die Bestimmung auch ausschließlich **manuell** erhobene, verarbeitete oder genutzte Beschäftigtendaten. Damit unterfallen dem Erlaubnistatbestand nahezu alle Tätigkeiten, die mit Informationen über den Beschäftigten zusammenhängen, wie etwa ein Anruf bei früheren Arbeitgebern, die Befragung und Beobachtung durch den Vorgesetzten, handschriftliche Aufzeichnungen über Leistungsverhalten oder Bewerbungs- bzw. Personalgespräche, aber auch eine Datenerhebung durch rein tatsächliches Handeln, wie etwa 32

Taschen-, Tor- oder Schrankkontrollen.[25] § 53 KDG findet damit prinzipiell auch auf **Personalakten in Papierform** Anwendung, soweit nicht spezielle kirchenrechtliche Bestimmungen zur Personalaktenführung der Auffangnorm des § 53 KDG vorgehen, vgl. § 2 Abs. 2 KDG.

### 3. Verhältnis zu anderen Vorschriften

33 Soweit **besondere kirchliche** oder **staatliche Rechtsvorschriften** auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften des KDG vor, § 2 Abs. 2 KDG. Regeln solche Spezialvorschriften einen Sachverhalt in beschäftigungsdatenschutzrechtlicher Hinsicht nicht abschließend, finden allerdings die **allgemeinen Bestimmungen des KDG** Anwendung. Stets im Blick zu behalten sind insbesondere die **Transparenzverpflichtungen** und **Betroffenenrechte**, namentlich das Recht auf Auskunft (§ 17 KDG), das Recht auf Berichtigung (§ 18 KDG) und das Recht auf Löschung (§ 19 KDG), wobei im Beschäftigungskontext eine modifizierte Anwendung geboten sein kann.

34 Dementsprechend enthält § 53 KDG **keine abschließende Verarbeitungsermächtigungsnorm** im kirchlichen Beschäftigtendatenschutz. Im Einzelfall kann auf die anderen Erlaubnistatbestände des KDG unter besonderer Berücksichtigung der Besonderheiten des kirchlichen Arbeitsrechts zurückgegriffen werden, namentlich auf die Erlaubnistatbestände des § 6 Abs. 1 KDG, § 8 KDG oder § 11 Abs. 2 KDG. So hat auch das BAG jüngst für das weltliche Beschäftigtendatenschutzrecht zu Recht angenommen, dass außerhalb des § 26 BDSG (§ 32 BDSG aF) ein Rückgriff auf Art. 6 DS-GVO zulässig sei.[26] Dies verdeutlicht, dass Beschäftigtendatenschutz in der Kirche sich einerseits zusammensetzt aus der Interessenabwägung im Rahmen des § 53 KDG, die im Wesentlichen durch die Rechtsprechung des BAG zum weltlichen Funktionsäquivalent (§ 26 BDSG bzw. § 32 BDSG aF) geprägt ist, andererseits aus den allgemeinen Vorschriften des KDG, die mit der DS-GVO in Einklang stehen. Erst durch dieses nicht immer einfache „Zusammenspiel" allgemeiner und spezifischer Regelungen lässt sich die Datenschutzkonformität einer Maßnahme im Einzelfall ermitteln.

## II. Datenverarbeitung vor Begründung eines Beschäftigungsverhältnisses

### 1. Allgemein zum Fragerecht des Arbeitgebers und zur Offenbarungspflicht des Beschäftigten

35 Die Frage, welche personenbezogenen Daten des Stellenbewerbers zulässigerweise erhoben werden dürfen, richtet sich nach den im Arbeitsrecht entwickelten **Grundsätzen zum Fragerecht des Arbeitgebers** unter Berücksichtigung der Besonderheiten des kirchlichen Dienstes.[27] Das führt an dieser Stelle zu einer engen Verschränkung von Arbeits- und Datenschutzrecht,[28]

25 ErfK/Franzen BDSG § 32 Rn. 2.
26 BAG 29.6.2017 – 2 AZR 597/16, Rn. 25.
27 In der datenschutzrechtlichen Literatur wird teilweise nicht von einem Fragerecht des Arbeitgebers, sondern von einem Informationserhebungsverbot gesprochen, das durch die Erlaubnisnorm des § 32 BDSG aF (jetzt: § 26 BDSG nF) durchbrochen werden muss und damit stets einer besonderen Rechtfertigung bedarf, vgl. in diesem Sinne Riesenhuber NZA 2012, 771 ff.
28 Joussen ZMV 2018, 118 (120).