Jahresbericht 2018

des Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

Berichtszeitraum
01.01.–31.12.2018

Katholisches
Datenschutzzentrum

Herausgegeben vom

Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn
sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und
Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands
(VDD)

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Hinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für beiderlei Geschlecht.

Bildnachweis Titelmotiv: istockphoto.com | matejmo

3. Jahresbericht

des Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

für den Zeitraum 01.01.2018– 31.12.2018

vorgelegt im April 2019

Redaktionsschluss: 12. April 2019

Inhaltsverzeichnis

Vorwort

Für das Katholische Datenschutzzentrum brachte das Jahr 2018 zwei Neuerungen.

Zum 01.01.2018 übernahm das Katholische Datenschutzzentrum auch die Datenschutzaufsicht über den Verband der Diözesen Deutschlands von der bisherigen Datenschutzaufsicht. Der Verband der Diözesen Deutschlands ist als Körperschaft des öffentlichen Rechts der Rechtsträger der Deutschen Bischofskonferenz. Diese zusätzliche Aufgabe haben wir 2018 in unsere Prozesse integriert.

Der große Umbruch in der Arbeit ergab sich aber am 24. Mai 2018. Mit Inkrafttreten des Gesetzes über den Kirchlichen Datenschutz (KDG) gilt nicht nur eine neue gesetzliche Grundlage, sondern es gelten auch neue Befugnisse für die kirchlichen Datenschutzaufsichten.

Auch wenn die Grundsätze des Datenschutzes durch das neue Gesetz im Vergleich zur bisherigen Gesetzeslage nicht geändert wurden, sieht das Gesetz einige Neuerungen vor, teilweise auch nur die ausführlichere Regelung schon bisher vorhandener Instrumente.

Das neue Gesetz, sowohl die Datenschutz-Grundverordnung (DSGVO) auf europäischer Ebene, als auch das nach Art. 91 DSGVO mit der europäischen Vorgabe in Einklang gebrachte Kirchliche Datenschutzgesetz, haben in den Monaten vor und nach der Anwendbarkeit des Gesetzes viel Kritik erfahren müssen. Sicherlich gibt es in dem Gesetz Ecken und Kanten, an denen in Ruhe und mit den Erfahrungen der praktischen Anwendung der Regelungen nochmal gefeilt werden sollte. Bei mancher Diskussion über die angeblichen Fehler und Ungereimtheiten der neuen Regelungen konnte man aber den Eindruck gewinnen, dass hier ein Gesetz, das ein „weiter so“ wie bisher behindert, diskreditiert werden soll.

„Das [Gesetz] hat in der kurzen Zeit seines Bestehens schon viel Kritik hinnehmen müssen.“ Dieses Zitat stammt aus dem Vorwort zur Veröffentlichung des ersten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz 1979, also mittlerweile vor 40 Jahren.

Dieser erste Bericht wurde noch nicht wie heute vom Bundesbeauftragten selbst herausgegeben, sondern erschien in der Reihe „Zur Sache“ als Veröffentlichung des Deutschen Bundestages mit einem Vorwort des Vorsitzenden des Innenausschusses des Deutschen Bundestages, Herrn Dr. Axel Wernitz. Weiter führt Dr. Wernitz aus, der Gesetzgeber habe sich die Fortentwicklung des Datenschutzrechts auch vorgenommen. Bevor aber eine Novellierung des Datenschutzgesetzes in Angriff genommen werde, sollten - so Dr. Wernitz - erst hinreichende Erfahrungen mit dem bestehenden Gesetz gesammelt werden, um „eine allzu kurzatmige Gesetzesproduktion“ zu vermeiden.

Diese Einschätzung aus dem Jahr 1979 nach einem Jahr Bundesdatenschutzgesetz erinnert sehr an aktuelle Diskussionen. Es lässt mich hoffen, dass sich heute wie damals die Einsicht durchsetzen wird, dass diese Regelungen angemessen und notwendig sind. Geben wir den neuen Gesetzen - sowohl der Europäischen Datenschutz-Grundverordnung wie auch dem Kirchlichen Datenschutzgesetz – die Chance, ihren guten und grundrechtswahrenden Ansatz in der Praxis nachzuweisen, bevor nach Änderungen am Gesetz gerufen wird. Manche in der Theorie erscheinende Schwachstelle stellt sich in der Praxis vielleicht als wenig gravierend heraus, berechtigte Anmerkungen müssen aber im Rahmen der Evaluation des Gesetzes aufgenommen werden.

„Geben wir den neuen Gesetzen die Chance, ihren guten und grundrechtswahrenden Ansatz in der Praxis nachzuweisen…“

Letztendlich geht es um den Grundrechtsschutz der Menschen, mit deren Daten kirchliche Stellen umgehen. Bei aller berechtigten Diskussion über die Reichweite des Grundrechts dürfen neue, bequeme und vermeintlich kostenlose oder kostengünstigere technische Möglichkeiten nicht zu einer Aushöhlung des Grundrechts führen.

Ein bewegendes und spannendes Erlebnis war auch die Teilnahme des Katholischen Datenschutzzentrums am Katholikentag in Münster. Die unzähligen Kontakte in diesen Tagen, die guten fachlichen Gespräche und die positive Resonanz, die wir zum Thema Datenschutz und zu unserer Präsenz auf dem Katholikentag bekommen haben, zeigen, dass unser Weg richtig ist, die direkte Kommunikation zu suchen.

Ich freue mich auf weiterhin spannende Diskussionen zum Datenschutz.

Steffen Pau
Diözesan- und Verbandsdatenschutzbeauftragter
und Leiter des Katholischen Datenschutzzentrums (KdöR)

1 Entwicklungen im Datenschutz

1.1 Entwicklungen in der Europäischen Union

Neben den noch nicht abgeschlossenen Beratungen zur ePrivacy-Verordnung gab es auf europäischer Ebene mehrere Gesetzgebungsvorhaben, die datenschutzrechtlichen Bezug haben.

1.1.1 Geltung der DSGVO ab 25. Mai 2018

Mit dem 25. Mai 2018 sind die Regelungen der Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, besser bekannt als Europäische Datenschutz-Grundverordnung (DSGVO), verbindlich anzuwenden. Sie enthält die europaweit einheitlichen grundlegenden datenschutzrechtlichen Bestimmungen. Nationale Gesetzgeber können im Rahmen der durch die DSGVO eröffneten Regelungsmöglichkeiten ergänzende Bestimmungen erlassen, wie dies der Bundesgesetzgeber mit dem Bundesdatenschutzgesetz (BDSG) umgesetzt hat. Die Mitgliedstaaten der Europäischen Union können aber nicht mehr die grundlegenden Bestimmungen der DSGVO abändern.

Damit endete die zweijährige Übergangszeit und die neuen Regelungen lösten die Richtlinie 95/46/EG ab, die in Deutschland durch das bis 24. Mai 2018 geltende Bundesdatenschutzgesetz umgesetzt worden war.

Mit der Anwendbarkeit der DSGVO nahm auch der Europäische Datenschutzausschuss (EDSA; engl. „European Data Protection Board" - EDPB) seine Arbeit auf. Sein Ziel ist es, auf europäischer Ebene die einheitliche Anwendung der DSGVO sicherzustellen. Darüber hinaus besitzt der EDSA beratende Funktion im Hinblick auf den Datenschutz betreffende politische und rechtliche Fragestellungen auf der Ebene der EU. Ferner kann der EDSA Leitlinien, Empfehlungen und Verfahren zu datenschutzspezifischen Fragestellungen erarbeiten. Eine seiner wesentlichen Aufgaben ist zudem die Abstimmung auf Ebene der Datenschutzaufsichten im Rahmen des sogenannten Kohärenzverfahrens. Dieses Verfahren soll eine einheitliche Rechtsanwendung, Gesetzesauslegung und Aufsichtspraxis im Bereich des Datenschutzes der EU sicherstellen.

Der EDSA besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats sowie dem Europäischen Datenschutzbeauftragten bzw. den jeweiligen Vertretern. Sofern in Mitgliedstaaten mehr als eine Aufsichtsbehörde für den Datenschutz zuständig ist, ist für diesen Mitgliedstaat ein gemeinsamer Vertreter zu benennen. Dies ist in der Bundesrepublik Deutschland mit Bundes- und Landesdatenschutzbeauftragten der Fall. Die Aufgabe des gemeinsamen Vertreters

wird nach den Vorgaben des BDSG durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) wahrgenommen.

Der gemeinsame Vertreter fungiert auch als Ansprechstation für die Aufsichtsbehörden der anderen Mitgliedstaaten, die so in jedem Fall einen Ansprechpartner in einem Nationalstaat erhalten, unabhängig von den ansonsten bestehenden Zuständigkeiten. Die Aufsichtsbehörden der anderen Nationalstaaten müssen nicht mehr den Aufwand betreiben, zunächst die zuständige Aufsicht in einem anderen Mitgliedstaat der EU ermitteln zu müssen.

„Der Europäische Datenschutzausschuss löste die nach der bisherigen EU-Richtlinie bestehende Art. 29-Gruppe ab."

Der Europäische Datenschutzausschuss löste die nach der bisherigen EU-Richtlinie bestehende Art. 29-Gruppe ab. Der Europäische Datenschutzausschuss machte sich auch umgehend einige der von der Art. 29-Gruppe verabschiedeten „Working Papers" zu eigen und verabschiedete diese als weitergeltende eigene Papiere.

1.1.2 Weitere Datenschutzregelungen auf Ebene der Europäischen Union

Die Richtlinie (EU) 2016/680 der Europäischen Union wurde zeitgleich mit der DSGVO beschlossen und regelt den Datenschutz in den Justiz- und Ermittlungsbehörden. Sie musste bis Anfang Mai 2018 in nationales Recht umgesetzt werden. Dies erfolgte in Deutschland mit der Neufassung des Bundesdatenschutzgesetzes.

Diese Richtlinie der EU ergänzt ebenso wie die Verordnung (EU) 2018/1725 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union die Datenschutz-Grundverordnung.

1.1.3 Weitere Beratungen zur ePrivacy-Verordnung

Der Entwurf der „Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)" sollte ursprünglich in zeitlichem Zusammenhang mit dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung (DSGVO) beraten und verabschiedet werden. Sie befindet sich aber immer noch im europäischen Gesetzgebungsverfahren. Wie bereits bei der DSGVO sind die Europäische Kommission, das Europäische Parlament und der Europäische Rat an dem Verfahren beteiligt. Zum Zeitpunkt der Erstellung dieses Jahresberichts ist noch nicht absehbar, wann eine Inkraftsetzung zu erwarten ist. Vor der Neuwahl des Europäischen Parlaments im Mai 2019 wird das Gesetzgebungsverfahren wohl nicht abgeschlossen werden können. Zielsetzung der neuen Verordnung ist die Ablösung der bisherigen E-Privacy-Richtlinie und die Regelung des bereichsspezifischen Datenschutzes für elektronische Kommunikation.

Derzeit können die sich aus der neuen Verordnung ergebenden Auswirkungen auf die verschiedenen Formen der Datenverarbeitung durch kirchliche Stellen noch nicht beurteilt werden.

1.1.4 Stärkung der Cybersicherheit auf europäischer Ebene

Am 10.12.2018 haben sich das Europäische Parlament, der Europäische Rat und die Europäische Kommission auf eine Stärkung der „Agentur der Europäischen Union für Netz- und Informationssicherheit" (ENISA) geeinigt und wollen ihr ein stärkeres Mandat geben.

Außerdem sollen die Bereiche Cybersicherheit und Datenschutz stärker verbunden werden und ENISA und die Datenschutzgremien auf europäischer Ebene stärker zusammenarbeiten.

1.2 Entwicklungen in der Bundesrepublik Deutschland

1.2.1 Neufassung des Landesdatenschutzgesetzes NRW

Am 17. Mai 2018 wurde im Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen das Gesetz zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs-und Umsetzungsgesetz EU - NRWDSAnpUG-EU) verkündet[1].

Mit diesem Gesetz wurde das Landesdatenschutzgesetz u.a. an die neue Rechtslage der Datenschutz-Grundverordnung angepasst.

1.2.2 Neufassung des Bundesdatenschutzgesetzes

Die Europäische Datenschutz-Grundverordnung gilt als europäische Verordnung zwar unmittelbar ohne nationales Umsetzungsgesetz. Sie gibt den Mitgliedsstaaten an einigen Stellen aber die Möglichkeit, die gesetzlichen Vorgaben zu spezifizieren oder weiterauszuführen, ohne den Verordnungstext vollständig zu wiederholen.

Der Bundesgesetzgeber ist dieser Aufgabe mit der Neufassung des Bundesdatenschutzgesetzes (BDSG) nachgekommen und hat die ausfüllenden Regelungen für die Datenschutz-Grundverordnung in der neuen Fassung des BDSG verbunden mit den notwendigen nationalen Umsetzungsregelungen für die Richtlinie (EU) 2016/680 für den Bereich der Justiz zusammengefasst.

Für die Kirche und die kirchlichen Datenschutzaufsichtsbehörden wichtig ist die Regelung des § 18 Abs. 1 Satz 4 BDSG.

1 GVBl NRW 2018, S. 244 ff.

§ 18 des neuen BDSG dient der besseren Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in der Bundesrepublik Deutschland. Ziel der Vorschrift ist zunächst, eine einheitliche Anwendung der DSGVO durch die oder den Bundesbeauftragten und die Aufsichtsbehörden der Länder sicherzustellen.

Die für die Kirchen relevante Regelung des § 18 Abs. 1 Satz 4 BDSG lautet: „Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach den Artikeln 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.".

Damit hat der Bundesgesetzgeber in Erfüllung der Vorgaben der DSGVO und unter Berücksichtigung der Besonderheiten der Kirchen (vgl. Art. 91 DSGVO) die Möglichkeit geschaffen, dass die kirchlichen Datenschutzaufsichten sich an der Willensbildung beteiligen und ihre Stellungnahme einbringen können, wenn die Kirchen von den nach § 18 BDSG behandelten Sachverhalten auch betroffen sind.

1.2.3 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DsAnpUG-EU)

Mit der Europäischen Datenschutz-Grundverordnung (DSGVO) gilt im Bereich der Europäischen Union (EU) ein einheitliches Datenschutzrecht. Um die dort enthaltenen Vorgaben vollumfänglich umzusetzen, waren die Gesetzgeber in Bund und Ländern gefordert, zur Vermeidung von gesetzlichen Widersprüchen oder Kollisionen zwischen DSGVO und nationalen Bestimmungen, erforderliche Anpassungen des nationalen Rechts vorzunehmen.

Nachdem der Bundesgesetzgeber in einem ersten Datenschutz-Anpassungs- und Umsetzungsgesetz unter anderem das Bundesdatenschutzgesetz an die neuen Regelungen der Datenschutz-Grundverordnung angepasst hatte, mussten mit dem zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz die vielen Fachgesetze angepasst werden, die Verweise auf das alte BDSG oder andere datenschutzrechtlich relevante Regelungen enthalten.

Mit diesem Artikelgesetz werden über 150 Einzelgesetze geändert und dadurch an die neuen datenschutzrechtlichen Vorgaben angepasst.

Stichwort: Artikelgesetz
Als Artikel- oder Mantelgesetz wird in der Gesetzgebungspraxis der Bundesrepublik Deutschland ein Gesetz bezeichnet, das gleichzeitig mehrere Gesetze oder sehr unterschiedliche Inhalte in sich vereint. Meist werden damit Änderungsgesetze bezeichnet, die eine bestimmte Thematik in einer ganzen Reihe von Rechtsgebieten ändern. Für diese Gesetze ist auch die Bezeichnung „Omnibusgesetz" gebräuchlich, wenn Änderungen, die inhaltlich nichts miteinander zu tun haben, in einem Artikelgesetz zusammengefasst werden.
Quelle: de.wikipedia.org/wiki/Artikelgesetz (abgerufen am 05.04.2019)

1.2.4 Gesetzentwurf zum Schutz von Geschäftsgeheimnissen

Mit der Richtlinie EU 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung sollen Geschäftsgeheimnisse europaweit besser geschützt werden.

Bislang ist der Geheimnisschutz in Deutschland uneinheitlich in verschiedenen Gesetzen geregelt. Diese Aufspaltung soll durch den Gesetzesentwurf vermieden werden. Erstmals soll es eine Legaldefinition von „Geschäftsgeheimnis" geben. Der Gesetzentwurf der Bundesregierung wird gegenwärtig im Deutschen Bundestag beraten (Drs 19/4724)[2].

1.2.5 Schutz vor Abmahnungen bei Datenschutzverstößen

Im Vorfeld der Anwendung der DSGVO wurde von Unternehmen befürchtet, dass von interessierten Stellen etwaige Umsetzungsmängel der neuen Regelungen, wie z.B. noch nicht oder nicht korrekt überarbeitete Datenschutzerklärungen für Internetseiten, großflächig mit Abmahnungen aufgegriffen werden könnten.

Auch wenn es bisher nur zu vereinzelten Abmahnungen kam und die befürchteten Abmahnwellen ausblieben, hat die Politik die Befürchtungen aufgegriffen und verschiedene Initiativen ergriffen, um Abmahnungen wegen datenschutzrechtlicher Verstöße zu verhindern[3].

Erste gerichtliche Entscheidungen äußern sich noch nicht einheitlich, ob durch die mit der DSGVO veränderte Rechtslage überhaupt Abmahnungen gegen datenschutzrechtliche Verstöße als wettbewerbsrechtliche Verletzungen möglich sind[4].

2 Der Deutsche Bundestag hat das Gesetz in dritter Lesung in seiner Sitzung am 21. März 2019 verabschiedet.
3 So z.B. die Initiative des Bundeslandes Bayern im Bundesrat (BR-Drs. 304/18) oder der Antrag von Bündnis 90/Die Grünen im Bundestag (BT-Drs. 19/6438). Beide Anträge sind noch in der parlamentarischen Beratung.
4 So z.B. Landgericht Würzburg, Beschluss vom 13.09.2018 (Az. 11 O 1741/18 UWG); a.A. z.B. Landgericht Wiesbaden Urteil vom 05.11.2018 (Az. 5 O 214/18).

Unabhängig von der Möglichkeit einer wettbewerbsrechtlichen Abmahnung besteht immer die Möglichkeit der Datenschutzaufsichten eine Verletzung datenschutzrechtlicher Pflichten zu beanstanden.

1.3 Entwicklungen in der römisch-katholischen Kirche

1.3.1 Gesetz über den Kirchlichen Datenschutz (KDG) in Kraft

Das Gesetz über den Kirchlichen Datenschutz (KDG) ist entsprechend dem einstimmigen Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands (VDD) vom 20. November 2017 mit Wirkung zum 24. Mai 2018 von den (Erz-)Diözesen in Deutschland in Kraft gesetzt worden[5].

Mit Inkrafttreten des KDG wurde die Anordnung über den kirchlichen Datenschutz (KDO) aufgehoben[6].

Bestehende Regelungen (außerhalb des KDG) mit datenschutzrechtlichen Bestimmungen müssen sich nun an den Vorgaben des KDG messen lassen, da gemäß § 2 Abs. 2 KDG andere kirchliche oder staatliche Rechtsvorschriften dem KDG nur vorgehen, sofern diese das Datenschutzniveau des KDG nicht unterschreiten.

In diesem Zusammenhang ist zu beachten, dass gemäß § 57 Absatz 5 KDG Verordnungen, die nach § 22 der Anordnung über den kirchlichen Datenschutz (KDO) erlassen wurden, insbesondere die Durchführungsverordnung zur KDO (KDO-DVO), zwar zunächst in Kraft bleiben, soweit sie den Regelungen des KDG nicht entgegenstehen. Das Gesetz sieht jedoch vor, dass sie nach Ablauf einer Übergangsfrist, die längstens bis zum 30. Juni 2019 festgelegt wurde, außer Kraft treten, sofern nicht bereits zuvor eine Neuregelung verabschiedet wird.

1.3.2 Kirchliche Datenschutzgerichtsordnung (KDSGO) in Kraft

Die Deutsche Bischofskonferenz hat mit Wirkung zum 24. Mai 2018 eine Kirchliche Datenschutzgerichtsordnung (KDSGO) erlassen.

Mit der KDSGO kommt die Katholische Kirche der Vorgabe aus § 49 KDG nach, im Einklang mit der Europäischen Datenschutz-Grundverordnung (DSGVO) für datenschutzrechtliche Sachverhalte einen wirksamen gerichtlichen Rechtsschutz zu gewährleisten.

5 Amtsblatt des Erzbistums Köln 2018, Nr. 12, S. 13 ff.; Kirchliches Amtsblatt für die Erzdiözese Paderborn 2018, Nr. 23 (S. 48 ff.); Kirchlicher Anzeiger für die Diözese Aachen vom 01.03.2018, Nr. 32, S. 78 ff.; Kirchliches Amtsblatt Bistum Essen 2018, Nr. 3 (S. 33 ff.); Kirchliches Amtsblatt für die Diözese Münster 2018, Art. 45 (S. 56 ff.); Amtsblatt für das Erzbistum München und Freising Nr. 9 vom 31. Mai 2018 für den Verband der Diözesen Deutschlands und die Dienststellen und Einrichtungen der deutschen Bischofskonferenz.

6 § 58 Abs. 1 KDG.

Der Rechtsweg in Datenschutzangelegenheiten sieht ein Verfahren mit zwei Gerichtsinstanzen vor. Die Bischöfe der (Erz-)Diözesen im Bereich der Deutschen Bischofskonferenz haben als erstinstanzliches Gericht ein Interdiözesanes Datenschutzgericht mit Sitz in Köln errichtet. Als zweite Instanz hat die Deutsche Bischofskonferenz ein Datenschutzgericht der Deutschen Bischofskonferenz mit Sitz in Bonn errichtet. Die Gerichte sind mit qualifizierten Richtern besetzt, die Erfahrungen unter anderem im Zivil- und Verwaltungsrecht, Datenschutzrecht und im kanonischen Recht besitzen.

„Der Rechtsweg in Datenschutzangelegenheiten sieht ein Verfahren mit zwei Gerichtsinstanzen vor."

Vor den Kirchlichen Gerichten in Datenschutzangelegenheiten stehen betroffenen Personen nunmehr gerichtliche Rechtsbehelfe gegen Verantwortliche oder kirchliche Auftragsverarbeiter zur Verfügung. Weiterhin können Entscheidungen der Datenschutzaufsicht in der Katholischen Kirche in Deutschland überprüft werden.

1.3.3 Die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) tritt am 01.03.2019 in Kraft

Nach den Vorgaben des Gesetzes über den Kirchlichen Datenschutz (KDG) konnte die aufgrund der bisherigen Anordnung über den Kirchlichen Datenschutz (KDO) erlassene Durchführungsverordnung (KDO-DVO) zunächst in Kraft bleiben, soweit sie nicht dem KDG entgegenstehende Regelungen enthält[7]. Jedoch war durch § 57 Abs. 5 KDG ein Auslaufen der Geltung der KDO-DVO zum 30. Juni 2019 vorgegeben.

Die vom Verband der Diözesen Deutschlands (VDD) erarbeitete Musterfassung der „Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)" wurde in der Vollversammlung des VDD am 19. November 2018 beschlossen. Als einheitliches Datum für das Inkrafttreten wurde der 1. März 2019 festgelegt.

Die Generalvikare der (Erz-)Diözesen haben die Verordnung für ihre jeweilige (Erz-)Diözese mit Wirkung ab dem 1. März 2019 in Kraft[8] und gleichzeitig die noch weitergeltende KDO-DVO außer Kraft gesetzt.

7 Die Konferenz der Diözesandatenschutzbeauftragten hat hierzu eine Arbeitshilfe „Weitergeltung der KDO-DVO unter dem KDG – Auslegung der Datenschutzaufsichten" herausgegeben.

8 Amtsblatt des Erzbistums Köln 2019, Nr. 43, S. 40 ff.; Kirchliches Amtsblatt für die Erzdiözese Paderborn 2018, Nr. 155 (S. 262 ff.); Kirchlicher Anzeiger für die Diözese Aachen vom 01.02.2019, Nr. 2, S. 27 ff.; Kirchliches Amtsblatt Bistum Essen 2019, Nr. 8 (S. 13 ff.); Kirchliches Amtsblatt für die Diözese Münster 2019, Art. 3 (S. 2 ff.); für den Verband der Diözesen Deutschlands und die Dienststellen und Einrichtungen der deutschen Bischofskonferenz wird die Veröffentlichung bis zum 30.06.2019 vorgenommen.

1.3.4 Weitere Gesetzgebungsvorhaben mit datenschutzrechtlichen Regelungen in der Katholischen Kirche

In einigen (Erz-)Diözesen in Deutschland gelten neben dem Gesetz über den Kirchlichen Datenschutz (KDG) bereichsspezifische Datenschutzregelungen, wie etwa für die Bereiche des Gesundheitsdatenschutzes und der Krankenhäuser sowie der Schulen.

Der Verband der Diözesen Deutschlands (VDD) hat den Wunsch der Diözesen, für den Patientendatenschutz eine den aktuellen Anforderungen des KDG und den Notwendigkeiten der katholischen Krankenhäuser entsprechende gesetzliche Regelung erlassen zu können, aufgegriffen und eine Unterarbeitsgruppe mit der Erarbeitung einer Musterfassung für ein Patientendatenschutzgesetz beauftragt. Die Unterarbeitsgruppe ist besetzt mit Fachleuten aus den katholischen Krankenhäusern, der Krankenhausseelsorge und dem Datenschutzrecht. Von Seiten des VDD wird die Vorlage eines Entwurfs für die Gremien des VDD im Jahr 2019 angestrebt.

Weiterhin ist der Wunsch nach Regelungen für den Schuldatenschutz geäußert worden.

Darüber hinaus wird vor dem Hintergrund der Vorgabe in § 58 Absatz 2 KDG, das am 24. Mai 2018 in Kraft getretene Gesetz innerhalb von drei Jahren zu überprüfen, von Seiten des kirchlichen Gesetzgebers rechtzeitig das entsprechende Verfahren einzuleiten sein.

1.4 Entwicklungen in der Evangelischen Kirche in Deutschland

Im Bereich der Evangelischen Kirche in Deutschland stellen sich beim Datenschutz vergleichbare Anforderungen und Fragestellungen wie bei der Katholischen Kirche. Die Evangelische Kirche in Deutschland (EKD) hat mit dem „Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland“ (DSG-EKD) ein dem KDG und der DSGVO vergleichbares Gesetz erlassen und somit die Vorgaben von Art. 91 DSGVO ebenfalls erfüllt. In der Anwendung des neuen Rechts ergeben sich vergleichbare Themen für die Beratung und Unterstützung der Einrichtungen vor Ort für die jeweiligen Datenschutzaufsichten.

Die EKD hatte sich bezüglich der Organisation der Datenschutzaufsicht schon unter der Geltung des alten Datenschutzrechts vor Mai 2018 dafür entschieden, mit dem „Beauftragten für den Datenschutz der EKD“ eine zentrale Stelle mit mehreren regionalen Zweigstellen zu schaffen. Es handelt sich dabei um eine Hauptstelle in Hannover mit den Zweigstellen in Hannover, Berlin, Ulm und Dortmund. Darüber hinaus haben einige Landeskirchen eigene Datenschutzaufsichten errichtet, da sie der zentralen Datenschutzaufsicht der EKD nicht beigetreten sind.

Die EKD hat zur Stärkung der Sicherheit der Datenverarbeitung eine Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung EKD – ITSVO-EKD) vom 29. Mai 2015 erlassen. Diese ist auch weiterhin in Kraft. Diese Verordnung legt u.a. für den Einsatz von IT fest, dass als Mindestvoraussetzungen für den Einsatz von IT ein Anforderungsprofil und eine Dokumentation vorliegen, die datenschutzrechtlichen Anforderungen eingehalten werden und die Systeme vor ihrem Einsatz getestet wurden.

1.5 Entwicklungen in der Datensicherheit

Durch das Inkrafttreten des Kirchlichen Datenschutzgesetzes und der Datenschutz-Grundverordnung im Mai 2018 bekam die Datensicherheit eine gesteigerte Aufmerksamkeit. Aber auch die anhaltenden Cyber-Angriffe haben das Bewusstsein für eine verbesserte Datensicherheit vergrößert.

Die erfolgreichen Angriffe auf die zentralen Prozessoren von Geräten, den CPUs, aller namenhaften Hersteller zeigen, dass alle Komponenten einer IT-Infrastruktur angreifbar und verwundbar sind. Forschung und Industrie stellen hierzu Technologien für die Verhinderung entsprechender Angriffsszenarien zur Verfügung.

Im Zuge von Beratungen und Informationsveranstaltungen des Katholischen Datenschutzzentrums wurde deutlich, dass einzelne Einrichtungen dem sehr komplexen Themengebiet nicht gewachsen sind. Zwar bringen moderne Betriebssysteme alle relevanten Sicherheitstechnologien mit sich, müssen aber entsprechend konfiguriert oder eventuell lizensiert werden. Hier kann eine Zentralisierung und ein Informationsaustausch der Verantwortlichen zielführend sein.

Das bisherige Paradigma „Never change a running System" hat in der heutigen schnelllebigen Zeit ausgedient. Nur durch ein schnelles Patch-Management lassen sich bekannte Sicherheitslücken schließen und so ein höheres Maß an Sicherheit erreichen.

1.5.1 Das Standard-Datenschutzmodell

Als „Standard-Datenschutzmodell“ (SDM) bezeichnen die deutschen Datenschutzaufsichtsbehörden eine Methode, mit der für den Bereich des operativen Datenschutzes sichergestellt ist, dass eine einheitliche Datenschutz-Beratungs- und Prüfpraxis in Bezug insbesondere zu den technisch-organisatorischen Maßnahmen der DSGVO bzw. den geltenden Rechtsnormen (wie dem KDG) erreicht werden kann. Mehrere Landesdatenschutzbeauftragte sowie der Beauftragte für den Datenschutz der EKD haben dazu an der Methode und an Maßnahmenkatalogen gearbeitet. Im Berichtszeitraum haben die Diözesandatenschutzbeauftragten überlegt, wie das Standard-Datenschutzmodell für die eigene Arbeit in Beratung und Prüfung genutzt werden kann. Derzeit laufen Überlegungen – auch zusammen mit den Datenschutzaufsichten der Evangelischen Kirche in Deutschland – zum weiteren Vorgehen und einer möglichen Umsetzung in die Beratungs- und Prüfungspraxis.

„Derzeit laufen Überlegungen (...) zu einer möglichen Umsetzung in die Beratungs- und Prüfungspraxis.“

Das Konzept des SDM sieht vor, die Gewährleistungsziele der DSGVO bzw. des KDG, in methodischer Anlehnung an IT-Grundschutz des BSI, um Schutzbedarfsfeststellungen zu ergänzen, um eine angemessene Skalierbarkeit der Auswahl und Wirksamkeit von Schutzmaßnahmen zu erreichen. Die Liste der Gewährleistungsziele (Vertraulichkeit, Verfügbarkeit, Integrität, Nichtverkettbarkeit, Transparenz, Intervenierbarkeit und – als übergeordnetes Ziel – Datenminimierung) werden in jeder Ebene der Verarbeitungstätigkeit (Daten, Systeme, Prozesse) entsprechend dem festgestellten Schutzbedarf durch einen vorformulierten Katalog an Schutzmaßnahmen unterstützt. In der Situation der Prüfung wird die Implementierung der Maßnahmen evaluiert, in der Situation der Beratung die passende Maßnahme empfohlen.

Der Schutzbedarf ist gekoppelt an den erwartbaren Schaden, der aus dem Risikoniveau einer Verarbeitung bzw. Verarbeitungstätigkeit herzuleiten ist. Im wesentlichen Unterschied zum Informationssicherheitsmanagement nimmt das SDM dabei die Perspektive der betroffenen Person ein, die es zu schützen gilt, und fokussiert sich primär auf die Minderung der Intensität des Grundrechtseingriffs bei natürlichen Personen. In einem zweiten Schritt werden dann die Grundrechtsverletzungen, die beispielsweise durch eine mangelhafte IT-Sicherheit entstehen können, beurteilt und durch Maßnahmen eingedämmt.

Konkrete Maßnahmenkataloge wurden bisher zu den Bereichen Aufbewahrung, Trennungsgebot, Löschen und Vernichten, Dokumentation, Protokollierung und zum Datenschutzmanagement veröffentlicht. Weitere Kataloge sind in Vorbereitung. Das Katholische Datenschutzzentrum wird die weitere Entwicklung des SDM positiv begleiten und unterstützen.

1.5.2 Verschlüsselung der Kommunikation

Der schnelle Austausch von Informationen gehört in der heutigen Zeit zum normalen Arbeitsalltag. Die elektronische Kommunikation bietet hier den Vorteil der schnellen Informationsübermittlung.

Die Einfachheit und Schnelligkeit der elektronischen Kommunikation darf aber nicht dazu führen, dass Überlegungen zum Schutz der Inhalte der Kommunikation, die uns bei Briefen oder Postkarten ganz natürlich erscheinen, bei der elektronischen Kommunikation per E-Mail oder Messenger nicht beachtet werden. Hier stellen wir in Gesprächen und Prüfungen vor Ort immer wieder fest, dass das Bewusstsein für den Schutz der Daten vor Verlust oder Manipulation nicht oder nicht in ausreichendem Maße vorhanden ist oder verdrängt wird. Daher ist von den Verantwortlichen u.E. ein entsprechendes Kommunikationskonzept zu erarbeiten, welches auf die Bedürfnisse der entsprechenden Teilnehmer und Inhalte der Kommunikation zugeschnitten ist.

Dabei wird nicht ein einziges Kommunikationsmittel die Lösung für alle Anwendungsszenarien sein können. Während einmal z.B. die kircheneigene Plattform Communicare die beste Lösung sein könnte, könnte es in einem anderen Fall die E-Mail sein. Dabei wird je nach Inhalt eine Absicherung der E-Mail unausweichlich sein[9].

9 Siehe hierzu auch die Anforderung in § 25 Abs. 1 KDG-DVO: „E-Mails, die personenbezogene Daten der Datenschutzklasse II oder III enthalten, dürfen ausschließlich im Rahmen eines geschlossenen und gesicherten Netzwerks oder in verschlüsselter Form mit geeignetem Verschlüsselungsverfahren übermittelt werden.".

2 Die Datenschutzaufsicht in der Katholischen Kirche

2.1 Struktur der Aufsichtsstellen

Die Datenschutzaufsicht in der Katholischen Kirche wird nicht von einer einzigen Stelle wahrgenommen. Vergleichbar den einzelnen Bundesländern mit eigener Gesetzgebung und jeweils eigenen Landesdatenschutzbeauftragten, hat auch jeder Diözesanbischof in Deutschland auf Grund seiner Gesetzgebungsgewalt das kirchliche Datenschutzrecht für die eigene (Erz-)Diözese in Kraft gesetzt und hat, wie im Gesetz vorgesehen, für den eigenen Wirkungskreis einen Diözesandatenschutzbeauftragten ernannt. Dieser Diözesandatenschutzbeauftragte nimmt die Funktion wahr, die im staatlichen Bereich der Landesdatenschutzbeauftrage als Datenschutzaufsicht wahrnimmt.

Zur effektiven und effizienten Wahrnehmung der Aufgaben der Datenschutzaufsicht und in Umsetzung des Urteils des Europäischen Gerichtshofes zur Unabhängigkeit der Datenschutzaufsichtsbehörden haben jeweils mehrere (Erz-)Diözesen gemeinsame Diözesandatenschutzbeauftragte als Datenschutzaufsicht bestellt. Die Verteilung ist in der nachfolgenden Übersicht dargestellt:

Datenschutzaufsichten der Katholischen Kirche Deutschlands

Daneben gibt es noch eine eigene Datenschutzaufsicht für die katholische Militärseelsorge, die in Personalunion vom Diözesandatenschutzbeauftragten für die ostdeutschen (Erz-)Diözesen wahrgenommen wird. Außerdem besteht eine eigenständige Datenschutzaufsicht für den Verband der Diözesen Deutschlands und die nachgeordneten Einrichtungen. Diese Aufsichtsfunktion wird in Personalunion vom Diözesandatenschutzbeauftragten für die nordrhein-westfälischen (Erz-)Diözesen wahrgenommen.

Für den Bereich der Ordensgemeinschaften päpstlichen Rechts hat die Deutsche Ordensobernkonferenz (DOK), der Zusammenschluss der Höheren Oberen der Orden und Kongregationen in Deutschland, die Einrichtung des Gemeinsamen Ordensdatenschutzbeauftragten der DOK als Datenschutzaufsicht geschaffen.

2.2 Konferenz der Diözesandatenschutzbeauftragten

Zu den Aufgaben des Diözesandatenschutzbeauftragten gehört gemäß §§ 44 Abs. 3 lit. f und 46 KDG das Hinwirken auf die Zusammenarbeit mit den anderen Diözesandatenschutzbeauftragten.

Um eine möglichst einheitliche Praxis bei der Auslegung des Gesetzes und bezogen auf Verfahrensabläufe der kirchlichen Stellen zu erreichen, tauschen sich die Diözesandatenschutzbeauftragten regelmäßig als Konferenz der Diözesandatenschutzbeauftragten aus. Neben den Diözesandatenschutzbeauftragten werden zu den Konferenzen auch die beiden von der Deutschen Ordensobernkonferenz bestellten Ordensdatenschutzbeauftragten für die päpstlichen Ordensgemeinschaften eingeladen. Beratend können noch weitere Vertreter (z. B. des Verbandes der Diözesen Deutschlands, des Katholischen Büros in Berlin oder der Deutschen Ordensobernkonferenz) an den Tagungen teilnehmen.

Die Beratungen dienen dazu, gemeinsame Standpunkte zu verabschieden und gemeinsame Vorgehensweisen zu Themen zu finden. Ziel ist die möglichst einheitliche Auslegung des KDG in allen deutschen (Erz-) Diözesen durch die kirchlichen Datenschutzaufsichten.

Im Berichtszeitraum fanden Konferenzen der Diözesandatenschutzbeauftragten im Februar und im April jeweils in Würzburg, im Juli in Dortmund und in Frankfurt und im Oktober in Bremen statt. Neben der Beratung aktueller Fragestellungen waren die Umsetzung der Anforderungen des neuen Datenschutzrechts für die kirchlichen Einrichtungen, aber auch für die Datenschutzaufsichten selbst wichtige Beratungspunkte der Sitzungen. Die Beschlüsse der Sitzungen sind in diesem Bericht in Kapitel 6 dokumentiert.

Auch zwischen den Tagungen stehen die Diözesandatenschutzbeauftragten in regelmäßigem Austausch über aktuelle Fragen.

Zur Vorbereitung technischer Sachverhalte hat die Konferenz der Diözesandatenschutzbeauftragten einen Arbeitskreis Technik ins Leben gerufen. Dieser Arbeitskreis wird vom stellv. Leiter des Katholischen Datenschutzzentrums geleitet.

Die katholischen und evangelischen Datenschutzaufsichten haben vor dem Hintergrund vergleichbarer Anforderungen und Fragestellungen beschlossen, sich regelmäßig über datenschutzrechtliche Themen auszutauschen und jährlich eine gemeinsame Sitzung der Konferenz der Diözesandatenschutzbeauftragten mit den evangelischen Datenschutzaufsichten durchzuführen. So trafen sich die Diözesandatenschutzbeauftragten mit den Datenschutzaufsichten der Evangelischen Kirche in Deutschland zum 2. Ökumenischen Datenschutztag im April 2018 in Erfurt.

„Auch zwischen den Tagungen stehen die Diözesandatenschutzbeauftragten in regelmäßigem Austausch über aktuelle Fragen."

2.3 FAQ zur Konferenz der Diözesandatenschutzbeauftragten

Zur Konferenz der Diözesandatenschutzbeauftragten werden immer wieder Fragen an uns herangetragen, die wir aus Sicht des Katholischen Datenschutzzentrums gerne beantworten möchten:

Auf welcher (Rechts-)Grundlage ist das Gremium der Konferenz der Diözesandatenschutzbeauftragen gebildet worden?

Das KDG gibt den Diözesandatenschutzbeauftragten in den §§ 44 Abs. 3 lit. f und 46 KDG das Hinwirken auf die Zusammenarbeit mit den anderen Diözesandatenschutzbeauftragten vor. Ein formales Gremium sieht das Gesetz aber nicht vor.

Die „Konferenz der Diözesandatenschutzbeauftragten" ist die von den Diözesandatenschutzbeauftragten selbst gewählte formalisierte Form dieser Vorgabe des KDG zur Zusammenarbeit.

Kann ich als Gast an den Sitzungen teilnehmen?

Die Konferenz besteht aus den Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen.

Durch die Beauftragung einzelner Diözesandatenschutzbeauftragter durch mehrere (Erz-)Diözesen gibt es derzeit fünf Diözesandatenschutzbeauftragte.

Als ständige Gäste nehmen die beiden von der Deutschen Ordensobernkonferenz bestellten gemeinsamen Ordensdatenschutzbeauftragten für die Datenschutzaufsichten der päpstlichen Ordensgemeinschaften an den Sitzungen teil, um auch hier die enge Abstimmung sicherzustellen.

Gemäß der Absprache in der Konferenz können themenbezogen oder zu einzelnen Sitzungen weitere Gäste eingeladen werden. Es besteht aber kein Anspruch einzelner Verbände oder Gremien auf Teilnahme an den Sitzungen.

Welche Verbindlichkeit / Rechtswirkungen haben die Beschlüsse der Konferenz?

Da die Konferenz kein gesetzlich vorgesehenes Gremium mit gesetzlichen Aufgaben und Befugnissen ist, können die Beschlüsse auch keine direkte bindende Wirkung per Gesetz entfalten.

Die Beschlüsse der Konferenz sind eine gemeinsame Auslegung der datenschutzrechtlichen Vorschriften und deren Anwendung auf bestimmte Sachverhalte durch die Diözesandatenschutzbeauftragten. Der Beschluss an sich ist daher für die kirchlichen Einrichtungen nicht verbindlich. Er entfaltet gegenüber den kirchlichen Stellen aber dadurch Wirkung, dass die eigene zuständige Datenschutzaufsicht den Beschluss zur Grundlage ihrer Entscheidung im konkreten Einzelfall machen wird, der dann für die Einrichtung verbindlich ist.

Der Wert der Beschlüsse ergibt sich daher u.E. daraus, dass es eine einheitliche Auslegung der Sachverhalte zwischen den Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen gibt. Für die kirchlichen Stellen bringen diese Beschlüsse aber auch ein großes Stück Berechenbarkeit der Datenschutzaufsichten, da sich die Einrichtungen an Hand der Beschlüsse auf die Entscheidung ihrer zuständigen Datenschutzaufsicht im konkreten Einzelfall besser einstellen können.

Zur Verbindlichkeit von Beschlüssen der Konferenz hat die Konferenz im Juli 2018 auch einen Beschluss gefasst[10].

Welche Funktion hat der Sprecher der Konferenz?

Die Konferenz wählt aus ihrer Mitte jährlich einen Sprecher. Aufgabe des Sprechers ist die Vorbereitung und Leitung der Sitzungen der Konferenz. Außerdem nimmt er in dem Jahr als Gast an der Ständigen Arbeitsgruppe Datenschutz- und Melderecht / IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands teil und nimmt andere Termine für die Konferenz wahr.

Wie kann ich mich direkt an die Konferenz wenden?

Die Konferenz der Diözesandatenschutzbeauftragten hat zur leichteren Erreichbarkeit eine „Geschäftsstelle" eingerichtet. Diese befindet sich beim Katholischen Datenschutzzentrum in Dortmund. Sie erreichen die Konferenz postalisch unter der Adresse des Katholischen Datenschutzzentrums in Dortmund oder per E-Mail ddsb@kdsz.de.

10 Siehe Beschluss „Rechtliche Qualität der Beschlüsse der Konferenz" vom 26.07.2018, abgedruckt in Kapitel 6 dieses Berichtes.

3 Aus der Tätigkeit des Datenschutzzentrums

3.1 Neue Zuständigkeit seit dem 01.01.2018 für den VDD

Ab dem 01.01.2018 ist der Diözesandatenschutzbeauftragte auch zugleich Verbandsdatenschutzbeauftragter des Verbandes der Diözesen Deutschlands und damit Datenschutzaufsicht über den Verband der Diözesen Deutschlands, den Rechtsträger der Deutschen Bischofskonferenz, und die dem VDD angegliederten Einrichtungen, wie z.B. das Kommissariat der Deutschen Bischöfe / Katholisches Büro in Berlin.

3.2 Aufgabenkatalog (Information - Beratung - Prüfung)

Die Aufgaben des Diözesandatenschutzbeauftragten bzw. des Verbandsdatenschutzbeauftragten des VDD als Datenschutzaufsicht sind im KDG bzw. im KDG-VDD beschrieben. Wer der Ansicht ist, dass bei der Verarbeitung von personenbezogenen Daten durch eine (katholische) kirchliche Stelle datenschutzrechtliche Regelungen verletzt worden sind, kann sich gemäß § 48 KDG bzw. KDG-VDD an die Datenschutzaufsicht wenden. Diese prüft den Sachverhalt und hört dazu die betroffene kirchliche Stelle an, soweit nach dem Vortrag ein Verstoß gegen datenschutzrechtliche Regelungen vorliegen könnte. Wichtig ist dabei das Benachteiligungsverbot des § 48 Abs. 3 KDG bzw. KDG-VDD: „Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an die Datenschutzaufsicht gewendet hat." Wer sich an die Datenschutzaufsicht wendet, darf daher keine Nachteile erleiden.

Die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben gehört nicht nur im Rahmen der Beschwerdebearbeitung, sondern als allgemeine Kernaufgabe zu den Tätigkeiten der Datenschutzaufsicht (vgl. § 44 Abs. 1 KDG).

§ 44 Abs. 3 lit. g) KDG ergänzt § 44 Abs.1 KDG. Danach soll die Datenschutzaufsicht „Untersuchungen über die Anwendung dieses Gesetzes durchführen, auch auf der Grundlage von Informationen einer anderen Datenschutzaufsicht oder einer anderen Behörde."

Auf Basis dieser Regelung kann und muss die Datenschutzaufsicht Überprüfungen auf Grundlage bei ihr eingehender Beschwerden vornehmen. Sie kann aber auch ohne den konkreten Bezug zu einer Beschwerde anlasslos prüfen, ob die Einrichtungen das Gesetz richtig anwenden[11].

11 Zur Auslegung der inhaltsgleichen Vorschrift des Art. 57 Abs. 1 lit. h DSGVO vgl. Selmayr in Ehmann/Selmayr, Kommentar DSGVO, 1. Aufl. 2017, Art. 57 Rn. 9 und Kugelmann/Buchmann in Schwartmann u.a., Heidelberger Kommentar DSGVO / BDSG, 1. Aufl. 2018, Art. 57 Rn. 74.

Für kirchliche Stellen im Sinne des § 3 Abs. 1 KDG macht § 44 Abs. 2 KDG nochmals deutlich, dass sie die Arbeit der Datenschutzaufsicht durch Auskünfte, Ermöglichung von Einsichtnahme in Akten und Räume zu unterstützen haben und Untersuchungen und Prüfungen zuzulassen haben. Den Anweisungen der Datenschutzaufsicht ist nach § 44 Abs. 2 lit. a) KDG Folge zu leisten.

Hierzu führt sie anlassbezogen, auf Grund der bei ihr eingehenden Beschwerden, oder ohne Anlass - im Rahmen regelmäßiger Kontrollen - Prüfungen zur Verbesserung des Datenschutzes durch. Hierbei spielt die Einhaltung der rechtlichen Vorgaben (Datenschutzrecht) ebenso eine Rolle wie die Umsetzung der notwendigen technisch-organisatorischen Schutzmaßnahmen gemäß den datenschutzrechtlichen Vorgaben (Datensicherheit). Beide Komponenten, die Umsetzung der rechtlichen Vorgaben und der technisch-organisatorischen Schutzmaßnahmen, müssen beachtet und umgesetzt werden, damit Datenschutz wirksam werden kann und die betroffenen Personen den gesetzlich vorgesehenen Schutz genießen können.

Kommt die Datenschutzaufsicht im Rahmen einer Prüfung oder der Bearbeitung einer Beschwerde zu dem Ergebnis, dass ein bestimmter von der kirchlichen Stelle durchgeführter oder unterlassener Vorgang bei der Verarbeitung personenbezogener Daten zu beanstanden ist, wird dies dokumentiert und dem Verantwortlichen schriftlich mitgeteilt. Je nach Schwere des Verstoßes gegen die datenschutzrechtlichen Vorgaben, kann das Katholische Datenschutzzentrum verschiedene Maßnahmen ergreifen, die bis zu einer Untersagung der konkreten Datenverarbeitung und der Verhängung eines Bußgeldes reichen können.

„Um datenschutzrechtlichen Verstößen vorzubeugen, steht das Team des Katholischen Datenschutzzentrums (...) beratend zur Verfügung..."

Um datenschutzrechtlichen Verstößen vorzubeugen, steht das Team des Katholischen Datenschutzzentrums im Rahmen seiner Aufgaben beratend zur Verfügung, um über die Anforderungen der datenschutzrechtlichen Regelungen zu informieren. Die Datenschutzaufsicht kann hier als Referent oder mit schriftlichen Informationen allgemeine Hinweise zur Umsetzung des Datenschutzes geben oder im Wege der Beratung im Einzelfall weiterhelfen.

Durch das Inkrafttreten des neuen KDG und die damit einhergehenden nötigen Veränderungen und Vorbereitungen gab es im Berichtszeitraum wie schon im zweiten Halbjahr 2017 einen großen Bedarf an Informationen, so dass das Katholische Datenschutzzentrum bei vielen Veranstaltungen kirchlicher Stellen Vorträge hielt, Gespräche mit Gremien und Arbeitskreisen führte und allgemeine Informationen schriftlich zur Verfügung stellte.

Bedingt durch die stetig zunehmende Sensibilisierung der kirchlichen Stellen und der betroffenen Personen für den Umgang mit personenbezogenen Daten, nahmen im Berichtszeitraum sowohl die Beratungs-

anfragen als auch die Beschwerden weiter zu. Seit der Geltung des KDG ist der Datenschutzaufsicht auch eine hohe Zahl von Datenschutzverletzungen nach § 33 KDG gemeldet worden.

3.3 (Vorort-)Prüfungen und Prozessaufnahmen

Neben den Prüfungen, die im schriftlichen Verfahren auf Grund von Beschwerden betroffener Personen durchgeführt wurden, hat das Katholische Datenschutzzentrum im Jahr 2018 auf Grund des enorm hohen Beratungsbedarfs und Informationsbedarfs zu den gesetzlichen Neuregelungen im Datenschutz keine anlasslosen Vorort-Prüfungen durchgeführt.

Auch in diesem Berichtszeitraum war allgemein festzustellen, dass die Umsetzung der gesetzlichen Vorgaben auf unterschiedlichem Niveau vorzufinden ist. Teilweise sind auch noch Aufgaben zu erledigen, die durch die nicht vollständige oder gar fehlende Umsetzung der alten Rechtslage noch offen sind und jetzt mit den neuen Regelungen umgesetzt werden müssen.

Dabei ist immer wieder erkennbar, dass nur die ausreichende Beschäftigung mit dem Thema und die damit verbundene Bereitstellung der notwendigen Ressourcen an verschiedenen Stellen (IT, Fachabteilungen, betrieblicher Datenschutz) die gewünschten Ergebnisse bietet. Die Umsetzung des Datenschutzes kann gelingen, wenn auf die Notwendigkeiten im Alltag der Einrichtung risikoorientiert mit Zeit und Mitteln reagiert werden kann und die Beschäftigung mit dem Thema durch Einbindung in die Prozesse der Einrichtungen zum normalen Tagesgeschäft wird.

Nach den Prozessaufnahmen in den fünf Generalvikariaten im vergangenen Berichtszeitraum führte das Katholische Datenschutzzentrum in diesem Berichtszeitraum eine zweitägige Prozessaufnahme beim Verband der Diözesen Deutschlands in Bonn durch. Im Rahmen dieser Prozessaufnahme wurde der Umgang mit personenbezogenen Daten an den verschiedenen Stellen dieser zentralen Kirchenverwaltung aufgenommen. Ziel war auch hier, die Struktur der Einrichtung und die verschiedenen Datenverarbeitungen in der Arbeit des VDD kennenzulernen. Durch die verschiedenen Gespräche, an denen auch die betriebliche Datenschutzbeauftragte teilnahm, ergab sich für das Katholische Datenschutzzentrum ein guter Einblick in die Arbeit mit personenbezogenen Daten des Verbandes. Es konnten auch viele Themen angesprochen werden und für die Fragen von Seiten des VDD Lösungen gefunden werden.

3.4 Beratungs- und Informationsbedarf durch das neue Gesetz

Durch das Inkrafttreten des Gesetzes über den Kirchlichen Datenschutz (KDG) zum 24. Mai 2018 ist der Beratungs- und Informationsbedarf der einzelnen kirchlichen Einrichtungen, aber auch von betroffenen Personen gestiegen. Die zuvor gültige Anordnung über den kirchlichen Datenschutz (KDO) wies im Vergleich zum KDG deutlich weniger Normen auf. Einige der neuen (zusätzlichen) Regelungen tragen zwar auch zum besseren Verständnis des Datenschutzes bei, da sie die Regelungen erläutern oder ausführlicher darstellen. Die Regelungen werden dadurch insgesamt aber komplexer.

Seitdem der Gesetzestext des KDG verfügbar ist, ist der Informationsbedarf sehr hoch und im Vergleich zu vorher deutlich gestiegen. Daher stellt das Katholische Datenschutzzentrum aktuelle Informationen auf der Homepage zur Verfügung. Gerade für einzelne, nun gesetzlich vorgeschriebene Neuerungen (z.B. die Benennung eines betrieblichen Datenschutzbeauftragten oder das Führen von Verzeichnissen von Verarbeitungstätigkeiten) sind auf der Homepage Praxishilfen vorhanden, welche eine ausführliche Information zu bestimmten Themen liefern und somit eine Hilfestellung darstellen. Darüber hinaus war es in 2018 eine wichtige Aufgabe des Katholischen Datenschutzzentrums, Beratungsanfragen zu beantworten und bei Veranstaltungen kirchlicher Einrichtungen, Arbeitskreise oder Verbände als Referent zum neuen KDG fachkundig zu beraten.

3.4.1 Benennung eines betrieblichen Datenschutzbeauftragten (bDSB)

Das KDG verpflichtet alle kirchlichen Stellen der verfassten Kirche, also Kirchengemeinden, Diözesen, Kirchenstiftungen und Gemeindeverbände, zur Benennung eines betrieblichen Datenschutzbeauftragten. Die gleiche Verpflichtung gilt für alle Einrichtungen z.B. der Caritas oder anderer kirchlicher Träger, sofern in der Regel mindestens 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind oder die Einrichtung mit der Verarbeitung von besonders sensiblen personenbezogenen Daten oder Daten zur systematischen Überwachung von Personen befasst ist. In der Praxis werden also die meisten kirchlichen Einrichtungen einen betrieblichen Datenschutzbeauftragten benennen müssen. Bei kleineren kirchlichen Vereinen und Verbänden sollte aber geschaut werden, ob die Voraussetzungen für eine Benennungspflicht wirklich gegeben sind.

Der betriebliche Datenschutzbeauftragte unterstützt den Verantwortlichen bei der datenschutzkonformen Gestaltung der Betriebsabläufe, z.B. bei der Einführung neuer Verfahren, aber auch bei der regelmäßigen Überprüfung der Einhaltung von Datenschutzbestimmungen oder der Durchführung von Mitarbeiterschulungen. Er ist auch Ansprechpartner für Mitarbeiter und externe betroffene Personen (Kunden, Gäste,

Dienstleister) in allen Fragen des Datenschutzes und unterliegt hierbei einer Verschwiegenheitspflicht, wenn ihm vertrauliche Sachverhalte anvertraut werden.

Nicht zuletzt ist er der Ansprechpartner der Aufsichtsbehörden und soll mit diesen zusammenarbeiten. Genau aus diesem Grund enthält das KDG die Bestimmung, dass der betriebliche Datenschutzbeauftragte der Datenschutzaufsicht zu melden ist. Das Katholische Datenschutzzentrum hat pünktlich zum Inkrafttreten des KDG am 24. Mai 2018 über seine Homepage ein Online-Formular zur Verfügung gestellt, über welches alle kirchlichen Einrichtungen ihre betrieblichen Datenschutzbeauftragten melden können. Die Eingaben werden direkt in eine zentrale Datenbank geleitet, die dem Katholischen Datenschutzzentrum zur Verfügung steht, um bei Anfragen oder Beschwerden zuerst den betrieblichen Datenschutzbeauftragten der betroffenen Stelle zu ermitteln und mit diesem in Kontakt treten zu können.

3.4.2 Bestandsaufnahme der Verarbeitungsprozesse mit personenbezogenen Daten

Die Bestandsaufnahme der in der Einrichtung vorhandenen Prozesse ist immer der erste Schritt zur Identifizierung derjenigen Prozesse, in denen personenbezogene Daten verarbeitet werden.

Hilfreich für die Einrichtungen ist hierbei, dass bereits nach § 3a KDO ein Verzeichnis aller Verfahren vorzuhalten war, in dem automatisierte personenbezogene Daten verarbeitet werden. In das Verzeichnis der Verarbeitungstätigkeiten nach § 31 KDG können nun ergänzend die Verfahren zugefügt werden, in denen der Verarbeitungsprozess manuell erfolgt. Im Abgleich mit einem evtl. bereits bestehenden Qualitätsmanagement kann hier der Fluss der Daten vom Zeitpunkt der ersten Erhebung in der Einrichtung über die eigentlichen Kernprozesse der jeweiligen Einrichtung bis hin zur Weitergabe von personenbezogenen Daten an Dritte verfolgt und so sichergestellt werden, dass kein (Teil-) Prozess der Verarbeitung personenbezogener Daten übersehen wird.

3.4.3 Überarbeitung bestehender Verträge zur Auftragsverarbeitung

Die Überarbeitung bestehender Verträge zur Auftragsverarbeitung in der Folge der Neuregelung durch das KDG wird fast immer erforderlich sein.

Unbeschadet der bisherigen Regelungen in der KDO legt das KDG dem Auftragnehmer eine Reihe neuer Verpflichtungen auf, die in die bestehenden Verträge mit aufgenommen werden müssen. So muss z.B. der Auftragnehmer den Verantwortlichen in seinen Verpflichtungen gemäß § 15 bis 25 KDG unterstützen. Entsprechende Regelungen müssen in bestehende Verträge übernommen werden.

Insbesondere bei Verträgen mit nichtkirchlichen Auftragsverarbeitern muss der kirchliche Auftraggeber darauf achten, seine Verpflichtungen aus dem KDG vertraglich auf den Auftragnehmer zu übertragen. Da für den Auftragnehmer selbst die DSGVO Anwendung findet, ist bei der Neuerstellung der Verträge darauf zu achten, dass diese Bindung für die Gültigkeit des KDG für alle datenschutzrechtlichen Belange im Zusammenhang mit der Einrichtung in die Verträge aufgenommen wird. Sollte der Vertrag nicht änderbar sein, sollte auf das kirchliche Datenschutzrecht auf andere geeignete Weise hingewiesen werden.

Ein weiterer wichtiger Regelungspunkt im Rahmen der Auftragsverarbeitung ist, ob die tatsächliche Datenverarbeitung innerhalb der Europäischen Union stattfindet, oder ob es sich um eine Datenverarbeitung in einem Drittland handelt. Eine Datenverarbeitung in einem Drittland ist nur dann zulässig, wenn durch die EU-Kommission festgestellt worden ist, dass es dort ein angemessenes Datenschutzniveau gibt. Einen solchen Angemessenheitsbeschluss der EU gibt es momentan nur für wenige Länder (Andorra, Argentinien, Kanada, Schweiz, Färöer-Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Uruguay). Bei allen anderen Drittländern ist eine Datenübermittlung grundsätzlich an ein vertraglich garantiertes Datenschutzniveau gebunden. Nur wenn dieses vorliegt, ist eine Datenübermittlung zulässig. Dieses garantierte Datenschutzniveau ist abhängig von dem jeweiligen Drittland.

Im Falle der USA gibt es eine Sonderregelung. Das zwischen der Europäischen Union und den USA vereinbarte „Privacy Shield" ist keine allgemeine Anerkennung des vergleichbaren Schutzniveaus, wie bei den anderen Ländern. Von diesem Abkommen können nur US-amerikanische Unternehmen profitieren, die sich dem Abkommen angeschlossen haben. Sofern sich ein US-amerikanisches Unternehmen auf diese Regelung beruft, muss der Auftraggeber prüfen, ob das Unternehmen am Privacy Shield teilnimmt.

Für alle anderen Unternehmen und andere Drittländer ist die Sicherstellung des geforderten Datenschutzniveaus durch die von der EU-Kommission vorgegebenen Standardvertragsklauseln herbeiführbar, wobei der Vorteil der Absegnung durch die EU-Kommission verloren geht, wenn Veränderungen an den Standardvertragsklauseln vorgenommen werden.

Die Anpassung der Verträge, die nach den Bestimmungen der KDO abgeschlossen sind, müssen gemäß der Übergangsfrist in § 57 Abs. 3 KDG bis zum 31.12.2019 abgeschlossen sein.

3.4.4 Umsetzung der (erweiterten) Betroffenenrechte und Informationspflichten

Die Betroffenenrechte spiegeln die Kernziele des Datenschutzes wieder und sind die wichtigsten Instrumente der betroffenen Personen im Schutzbestreben bezüglich der eigenen Daten. Die im KDG formulierten Informationspflichten sind daher von entscheidender Bedeutung, damit die betroffenen Personen aufgeklärte Entscheidungen treffen können.

„Die Betroffenenrechte spiegeln die Kernziele des Datenschutzes wieder..."

Wichtig ist, dass diese Informationen leicht zugänglich und transparent sind. Die Bedeutung des Transparenzgebots wird im KDG durch die in §§ 14 ff KDG konkretisierten Vorschriften deutlich. Die zugänglich gemachten Informationen müssen präzise sein. Dieses Erfordernis wird erfüllt, wenn sie vollständig, aber auf das Wesentliche beschränkt sind.

Entscheidend ist zudem der Zeitpunkt. Die Information muss vor Beginn der ersten Verarbeitungstätigkeit erfolgen. Nur auf diese Weise ist sichergestellt, dass die betroffenen Personen sich über die Bedeutung der Datenverarbeitung und die möglichen Konsequenzen bewusst sind.

Der Umfang des Inhalts der Informationspflicht wird durch die Regelungen in §§ 15 und 16 KDG bestimmt. Bewertungsfaktor ist die Verständlichkeit der Formulierungen. Hierfür können wohl die Grundsätze herangezogen werden, die für Allgemeine Geschäftsbedingungen entwickelt wurden.

Schwierig wird es, wenn den betroffenen Personen die Ausübung Ihrer Rechte erschwert wird, in dem zusätzliche Forderungen aufgestellt werden. So kann z.B. das Recht auf Auskunft gemäß § 17 KDG nicht von einer Begründung, wofür die Daten benötigt werden abhängig gemacht werden.

Der Anspruch auf Berichtigung nach § 18 KDG richtet sich auf unrichtige verarbeitete personenbezogene Daten. Richtig oder unrichtig können nur Tatsachen sein, dh. dem Beweis zugängliche Vorgänge oder Zustände, nicht aber Werturteile. Für den Berichtigungsanspruch kommt es nicht auf den Umfang oder die Ursache der Unrichtigkeit an.

Sofern die Ansprüche der betroffenen Personen nicht oder nicht ausreichend gewährt werden, kann die betroffene Person ihre Ansprüche mit Hilfe der Datenschutzaufsicht durchsetzen.

3.4.5 Verzeichnis von Verarbeitungstätigkeiten - neue Bezeichnung für bekannte Inhalte

Bisher sah § 3a KDO vor, dass die verantwortliche Stelle ein Verzeichnis der Verfahren automatisierter Verarbeitung vorhalten und auf Anfrage jedermann zugänglich machen musste.

Diese Anforderung nach dem Verfahrensverzeichnis findet sich nun – nach der Anpassung der kirchlichen Regelungen an die DSGVO – in § 31 KDG als Verzeichnis von Verarbeitungstätigkeiten.

Durch die ergänzten Anforderungen an das Verzeichnis ergibt sich ein Anpassungsbedarf für die bestehenden Verzeichnisse. Für diese Änderungen oder Ergänzungen hat der Gesetzgeber in § 57 Abs. 4 KDG eine Frist bis zum 30.06.2019 vorgesehen. Sollte entgegen § 3a KDO noch kein Verfahrensverzeichnis bestanden haben, ist das Verzeichnis nach § 31 KDG ebenfalls bis zum 30.06.2019 zu erstellen.

In der Beratungspraxis haben sich durch diese Änderungen eine Vielzahl von Anfragen und ein erhöhter Beratungsbedarf ergeben. Eine Vielzahl von Anfragen konzentrierte sich auf die Änderungen im Vergleich zu den Regelungen in § 3a KDO.

Weiterhin bestanden Unklarheiten darüber, inwieweit nicht nur der Verantwortliche selber, sondern auch die Auftrags- und Unterauftragsverarbeiter ein Verzeichnis zu erstellen haben. Ein weiterer stark nachgefragter Bereich ist die geforderte allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 26 KDG.

Die Verzeichnisse sind nach den Regelungen des KDG dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen. Neu mit Einführung des KDG ist, dass diese Verpflichtung sowohl den Verantwortlichen als auch die Auftragsverarbeiter trifft.

Im Gegensatz zu § 3a Abs. 4 KDO sieht § 31 KDG keine Verpflichtung mehr vor, das Verzeichnis auf Anfrage jedermann zugänglich zu machen. Auch muss das Verzeichnis – sofern kein betrieblicher Datenschutzbeauftragter benannt ist – nicht mehr unaufgefordert der Datenschutzaufsicht gemeldet werden. Stattdessen muss das Verzeichnis dem Diözesandatenschutzbeauftragten nun auf Anforderung vorgelegt werden.

Zum Thema Verzeichnis von Verarbeitungstätigkeiten hat das Katholische Datenschutzzentrum eine Formulierungshilfe inklusive Musterverzeichnis erarbeitet und im Dezember 2018 veröffentlicht. Das zur Verfügung gestellte Muster enthält einen Teil, der in jedem Fall auszufüllen ist und die Mindestanforderungen des Gesetzes wiedergibt.

Darüber hinaus enthält das Muster Empfehlungen, welche Daten noch in das Verzeichnis aufgenommen werden könnten. Durch diese ergänzenden Angaben könnte das Verzeichnis von Verarbeitungstätigkeiten als zentraler Dokumentationsstand für die Erfüllung der Dokumentationsplicht z.B. aus § 7 Abs. 2 KDG („… und muss dies nachweisen können.“) genutzt werden.

3.4.6 Datenschutz-Folgenabschätzung

Bei der Neueinführung von Verfahren automatisierter Verarbeitungen von personenbezogenen Daten war auch nach der bisherigen Rechtslage nach § 3 Abs. 5 KDO eine Prüfung des Risikos vorzunehmen, das für die personenbezogenen Daten durch die geplante Verarbeitung entsteht und dieses Risiko anschließend zu minimieren (Vorabkontrolle). Mit Inkrafttreten des KDG wurde die Vorabkontrolle durch die Datenschutz-Folgenabschätzung (DSFA) in § 35 KDG abgelöst.

Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn Verfahren der Datenverarbeitung neu eingeführt oder wesentlich geändert werden, die mit einem voraussichtlich hohen Risiko für die betroffenen Personen behaftet sind.

Die DSFA ist eine begleitende Maßnahme zur Einführung der neuen Verarbeitung, mit der der Verantwortliche sicherstellt, dass das neue Verfahren von Anfang an („Datenschutz by Design“) datenschutzkonform aufgestellt wird. Die Durchführung der DSFA und die Umsetzung ihrer Ergebnisse ist also normalerweise personell und organisatorisch in das Vorhaben eingebettet.

Der Inhalt einer DSFA ist im § 35 Abs. 7 KDG nur mit Mindestanforderungen beschrieben. Im Kern handelt es sich um ein eigenes „Risiko-Management-System“, in dessen Fokus aber nicht die Risiken für den Erfolg des Vorhabens oder die wirtschaftlichen Risiken für den Verantwortlichen stehen, sondern die Risiken für die Rechte und Freiheiten der durch das Vorhaben betroffenen natürlichen Personen. Diese Risiken sind entsprechend der klassischen Risiko-Management-Methodik zu identifizieren, zu bewerten, durch geeignete Maßnahmen abzustellen oder auf ein vertretbares Maß (gemäß Risikoeinschätzung) zu mildern und zu überwachen.

Im Ergebnis kann die DSFA zu einer Modifikation des geplanten Verfahrens führen, um das Verfahren datenschutzkonform betreiben zu können. Nötigenfalls ist die Datenschutzaufsicht zu Konsultationen hinzuzuziehen. Im Extremfall kann das Ergebnis auch sein, dass das geplante Verfahren auch unter Modifikationen oder Realisierung zusätzlicher Datenschutzmaßnahmen auf keinen Fall datenschutzkonform gestaltet werden kann und deshalb unterbleiben muss.

Im Jahr 2018 hat das Katholische Datenschutzzentrum zusammen mit den anderen katholischen Datenschutzaufsichten gemäß § 35 Abs. 5 KDG eine Liste von Verarbeitungsvorgängen veröffentlicht, bei denen eine Datenschutz-Folgenabschätzung immer durchzuführen ist, da in diesen Fällen durchweg von einem voraussichtlich hohen Risiko für die betroffenen Personen auszugehen ist. Die Liste wurde als Beschluss der Konferenz der Diözesandatenschutzbeauftragten veröffentlicht[12] und orientiert sich an den Kriterien der Artikel-29-Gruppe, dem Vorläufer des Europäischen Datenschutzausschusses als Zusammenschluss aller nationalen Datenschutz-Aufsichtsbehörden in der EU.

3.4.7 Katholisches Datenschutzzentrum stellt Meldeplattform zur Verfügung

Das Kirchliche Datenschutzgesetz sieht in § 33 KDG eine Meldung von Datenschutzverletzungen bei der Datenschutzaufsicht vor. Weiterhin sieht § 36 KDG eine Meldung von benannten betrieblichen Datenschutzbeauftragten bei der Datenschutzaufsicht vor.

„Unter der Federführung des Katholischen Datenschutzzentrums konnte die Meldeplattform kurzfristig und rechtzeitig (...) zur Verfügung gestellt werden."

Um den meldenden Stellen eine einfache Möglichkeit zur Abgabe der Meldung zu schaffen, aber auch um als Datenschutzaufsicht die eingehenden Meldungen besser verarbeiten zu können, haben die Diözesandatenschutzbeauftragten die Einführung einer elektronischen Meldemöglichkeit für beide Fälle abgesprochen.

Unter der Federführung des Katholischen Datenschutzzentrums konnte die Meldeplattform mit einem engagierten Partner kurzfristig und rechtzeitig zum Start des neuen Gesetzes zur Verfügung gestellt werden. Die Plattform wird ständig weiterentwickelt und den aktuellen Anforderungen angepasst.

3.4.8 Wirtschaftlichkeit technisch-organisatorischer Maßnahmen nach § 26 KDG

Das Kirchliche Datenschutzgesetz verlangt nicht, dass jede Verarbeitung personenbezogener Daten den gleichen technisch-organisatorischen Maßnahmen zum Schutz der Daten unterworfen wird.

Das Gesetz will in § 26 Abs. 1 KDG ausdrücklich eine risikoorientierte Betrachtung der Verarbeitung der Daten und davon abgeleitete angemessene technische und organisatorische Schutzmaßnahmen „unter Berücksichtigung unter anderem des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen".

12 Siehe Kapitel 6 dieses Berichtes.

Die Nennung der Implementierungskosten erlaubt dabei auch die Berücksichtigung wirtschaftlicher Aspekte im Rahmen dieser Abwägung. Dies bedeutet, dass bei zwei gleich wirksamen Maßnahmen zum Schutz der Daten bei der konkreten Verarbeitung nicht die Umsetzung der teureren Maßnahme verlangt werden kann.

Die Umsetzung einer notwendigen Schutzmaßnahme kann aber auch nicht einfach unter Hinweis auf ein fehlendes oder niedrigeres Budget verweigert werden. Arbeitet ein Verantwortlicher mit personenbezogenen Daten und führt diese Verarbeitung zu einer Gefahr für die Rechte und Freiheiten der betroffenen Personen, muss er dieser Gefahr mit angemessenen Mitteln begegnen. Gradmesser für die Notwendigkeit einer Maßnahme ist das quantitative Risiko, dass der Verantwortliche mit der Verarbeitung für die betroffene Person schafft und nicht die Höhe des zur Verfügung stehenden Budgets für solche Maßnahmen. Würde die Höhe des zur Verfügung stehenden Budgets allein als Argument ausreichen, könnten die Verantwortlichen mit der vorherigen Festlegung von extrem niedrigen Budgets für die Maßnahmen das Schutzniveau bestimmen und eben keine risikoorientierte Betrachtung des Einzelfalls vornehmen.

§ 26 Abs. 3 KDG betont den Grundsatz der Wirtschaftlichkeit nochmals mit dem Hinweis auf die Verhältnismäßigkeit von Aufwand und angestrebten Schutzzweck und unterstreicht damit die oben genannten Ausführungen.

3.5 Einzelne Themen beleuchtet

Im Folgenden greifen wir einige Themenbereiche aus Beratung und Prüfung auf, da diese Sachverhalte u.E. Bedeutung über den Einzelfall hinaus haben.

3.5.1 Auftragsverarbeitung und das andere Rechtsinstrument

Erbringt eine kirchliche Stelle für eine andere kirchliche Stelle Dienstleistungen bei der Verarbeitung personenbezogener Daten und handelt es sich dabei um zwei eigenständige Verantwortliche im Sinne des Datenschutzes, dann ist für die Verarbeitung der Daten des einen Verantwortlichen durch den anderen Verantwortlichen eine Rechtsgrundlage notwendig.

In vielen Fällen wird eine Auftragsverarbeitung im Sinne des Datenschutzes vorliegen, so dass ein entsprechender Vertrag mit dem in § 29 KDG genannten Inhalt abzuschließen ist. Die datenverarbeitende kirchliche Stelle wird damit zum Auftragnehmer der Auftragsverarbeitung der anderen kirchlichen Stelle, welche verantwortlich für die Verarbeitung der personenbezogenen Daten ist.

Dies ist aber keine Neuerung des seit Ende Mai 2018 geltenden Kirchlichen Datenschutzgesetzes, sondern ergab sich auch schon vorher aus § 8 KDO.

Da im kirchlichen Bereich zentrale Stellen wie z.B. die Diözese gleichartige Dienstleistungen für viele andere kirchliche Stellen anbieten wie z.B. die Kirchengemeinden, müssen zwischen dem Erbringer der Leistung, im Beispiel die Diözese, und jedem Empfänger der Leistung einzelne Verträge zur Auftragsverarbeitung abgeschlossen werden.

Das KDG bietet in § 29 KDG für solche Sachverhalte nun die Möglichkeit an, statt eines einzelnen Vertrages ein sogenanntes „anderes Rechtsinstrument“ zu nutzen. Dieses „andere Rechtsinstrument“ soll insofern eine Erleichterung bringen, als der Leistungserbringer, im Beispiel die Diözese, durch formellen Rechtsakt, der alle (potentiellen) Leistungsempfänger bindet, die Einzelheiten der Verarbeitung regelt und die Leistungsempfänger dieser Verarbeitung dann nur noch beitreten müssen. Der formelle Rechtsakt muss aber alle Inhalte enthalten, die sonst auch Gegenstand des Vertrages zur Auftragsverarbeitung gewesen wären. Daran wird auch deutlich, dass für jede Auftragsverarbeitungssituation ein eigenes Rechtsinstrument zu schaffen ist, wie auch ein eigener Auftragsverarbeitungsvertrag für jede Auftragsverarbeitung abzuschließen ist.

3.5.2 Anfertigung und Veröffentlichung von Fotografien unter dem KDG

Die datenschutzrechtlichen Fragen rund um die Veröffentlichung von Fotografien war eines der meistdiskutierten Themen im Berichtszeitraum.

Bei diesem Thema gibt es derzeit aber noch offene Fragen zur (vorrangigen) Anwendbarkeit gesetzlicher Regelungen vor der DSGVO bzw. dem KDG. Daher ist hier noch vieles in der Diskussion. Dabei ist zu beachten, dass es sich bei dem vieldiskutierten Kunsturhebergesetz (KUG) um ein Gesetz aus dem Jahre 1907 handelt, dessen Regelungen die Veröffentlichung von Bildern im Internet und die damit verbundenen Möglichkeiten und Risiken nicht mit einbezogen hat.

Die Konferenz der Diözesandatenschutzbeauftragten hat zum Schutz der Kinder und Jugendlichen trotz dieser bestehenden Unsicherheiten beschlossen, „dass zumindest für die Veröffentlichung von Bildern von Kindern bis zur Vollendung des 16. Lebensjahres die vorherige Einwilligung der Sorgeberechtigten unter Vorlage der jeweils zur Veröffentlichung vorgesehenen Bilder einzuholen ist."[13] Personenbezogene Daten von Kindern und Jugendlichen genießen durch die Regelungen des KDG einen besonderen Schutz. Dieses besondere Schutzniveau wird ebenfalls in der DSGVO erwähnt. Daher ist bei der Veröffentlichung von Aufnahmen Minderjähriger bis zur Vollendung des sechzehnten Lebensjahrs die Einwilligung der Personensorgeberechtigten einzuholen.

Bisher konnte sich die Stelle, welche ein Foto veröffentlicht, in vielen Fällen auf das Kunsturhebergesetz berufen. Danach konnte ein Bildnis der Zeitgeschichte, eine Person, die nur als Beiwerk auf einem Foto auftaucht, eine Versammlung oder ähnliche Veranstaltung oder künstlerische Darstellungen auch ohne Einwilligung veröffentlicht werden (§ 23 Abs. 1 KUG).

Die zukünftige Anwendbarkeit des Kunsturhebergesetzes bzw. einzelner Regelungen daraus aufgrund eines möglichen Vorrangs der Regelungen der DSGVO und damit des KDG ist zumindest noch nicht abschließend geklärt und daher als nicht sichere Rechtsgrundlage zu bewerten.

Auch nach der DSGVO ist zwar grundsätzlich eine konkludente Einwilligung möglich, jedoch aufgrund von Beweiszwecken nicht empfehlenswert. Daher ist in § 8 Abs. 2 S. 1 KDG auch die Schriftform als generell erforderlich angegeben. Rein informativ sei darauf hingewiesen, dass eine Einwilligung im Sinne des § 22 S. 1 KUG gemäß § 107 BGB der Einwilligung der Personenfürsorgeberechtigten bedarf, insofern die betroffene Person noch nicht die volle Geschäftsfähigkeit erreicht hat. Art. 6 Abs. 1 lit. f DSGVO gilt dann als Rechtfertigung für Aufnahmen

13 Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 17.04.2018, siehe Kapitel 6 dieses Berichtes. Die Konferenz wird sich im April 2019 erneut mit der Thematik beschäftigen und den bestehenden Beschluss überarbeiten.

eines Fotografen, wenn seine Tätigkeit dem Kunstbegriff unterfällt. Dies gilt jedoch nur für die Aufnahmen, nicht für Veröffentlichungen. So nimmt auch der Hamburgische Landesdatenschutzbeauftragte in einem Vermerk Stellung zur Rechtfertigung bezüglich der Anfertigung von Fotoaufnahmen. „Eine solche Rechtfertigung kann hier nicht dem KUG entnommen werden“[14]. Das Kunsturhebergesetz bezieht sich nur auf Veröffentlichungen.

Wenn kirchliche Stellen personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeiten, gilt das Einwilligungserfordernis nicht, da hier das sogenannte Presseprivileg nach § 55 KDG greift. Jedoch ist mit dieser „Erlaubnisnorm“ vorsichtig umzugehen. So kann oft fraglich sein, ob die Umstände der Veröffentlichung eines Bildes journalistisch-redaktionell geprägt sind und eine meinungsbildende Funktion haben. Daher wird bei vielen kirchlichen Funktionen im konkreten Fall zu prüfen sein, ob diese Voraussetzungen vorliegen oder nicht.

3.5.3 Bring-Your-Own-Device (BYOD)

Das Thema „Bring Your Own Device“ ist im vergangenen Jahr Gegenstand verschiedener Anfragen geworden. Hierunter versteht man die dienstliche Nutzung privater Kommunikationsgeräte (Smartphone, Laptop, Tablet usw.). Dabei ergeben sich datenschutzrechtliche Herausforderungen, die vor einer Verarbeitung dienstlicher Daten auf privaten Geräten gelöst werden müssen.

Wenn die kirchliche Einrichtung den Mitarbeitenden die Möglichkeit gibt, über ihr privates Smartphone dienstliche E-Mails zu empfangen oder mit dem privaten Laptop von zu Hause auf die dienstlichen Laufwerke und damit auf die Dateien zuzugreifen, dann erscheint dies erstmal als Vorteil für beide Seiten. Auch in diesen Konstellationen muss die kirchliche Einrichtung als Verantwortlicher für die ordnungsgemäße Verarbeitung der personenbezogenen Daten aber immer sicherstellen, dass der Schutz der Daten gewährleistet ist.

Wenn also z.B. auf einem dienstlichen Smartphone im Falle des Verlustes die automatisierte Löschung aller Daten vorgesehen ist, wie wird dies bei dem Einsatz eines privaten Gerätes sichergestellt? Wenn Mitarbeitende Dateien aus dem dienstlichen Netzwerk herunterladen, wie stellt die kirchliche Einrichtung sicher, dass der Schutz der Daten auf dem privaten Gerät im gleichen Umfang gewährleistet ist, wie im internen Netzwerk bzw. auf einem dienstlichen Gerät mit entsprechenden Schutzmaßnahmen?

Die Durchführungsverordnung zur Anordnung über den Kirchlichen Datenschutz (KDO-DVO), die gemäß § 57 Abs. 5 KDG im Berichtszeitraum noch weiter anwendbar war, sieht in Abschnitt IV. (zu § 6 KDO)

14 Vermerk des Hamburgischen Beauftragten für Datenschutz und Informationssicherheit - https://datenschutz-hamburg.de/assets/pdf/Vermerk_Fotografie_DSGVO.pdf.

in der Anlage 3 unter Punkt 4.3 die Verarbeitung dienstlicher Daten in vorab zu begründenden und zu genehmigenden Ausnahmefällen auf privaten Datenverarbeitungsanlagen vor, soweit die dort genannten Bedingungen eingehalten werden.

Zumindest für die Nutzung privater Geräte der Mitarbeitenden im Homeoffice bzw. von privaten Laptops bei mobiler Arbeit könnten je nach Einzelfall auch noch die Regelungen der KDO-DVO in Abschnitt IV. (zu § 6 KDO) in der Anlage 2 unter Punkt 5.1 herangezogen werden. Diese besagen, dass die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungssystemen zu dienstlichen Zwecken grundsätzlich unzulässig ist. Ausnahmen können in schriftlich zu begründenden Ausnahmefällen vom Dienststellenleiter genehmigt werden. Ergänzt wird diese Regelung noch durch die Regelung in Abschnitt IV. (zu § 6 KDO) in der Anlage 2 unter Punkt 3.4, der eine ausschließliche Nutzung dienstlicher autorisierter Programme aus dienstlich genutzten Anlagen der elektronischen Datenverarbeitung vorsieht. Die Benutzung privater Programme ist nach dieser Regelung ausdrücklich unzulässig.

In der neu erlassenen KDG-DVO richtet sich die Nutzung privater IT-Systeme zu dienstlichen Zwecken ab März 2019 nach den Vorschriften des § 20 KDG-DVO. Die Verarbeitung von personenbezogenen Daten auf privaten IT-Systemen ist auch mit der Neuregelung nur innerhalb der in § 20 Abs. 2 KDG-DVO festgelegten Parameter zulässig.

Eine Möglichkeit, die die Nutzung privater Geräte auch aus Sicherheits- und Datenschutzgründen ermöglichen würde, ist der Einsatz von speziellen Container-Lösungen auf den Geräten, mit denen private und betriebliche Daten getrennt werden können.

„Eine Möglichkeit, die die Nutzung privater Geräte (...) ermöglichen würde, ist der Einsatz von (...) Container-Lösungen (...), mit denen private und betriebliche Daten getrennt werden können."

3.5.4 Datenschutz bei Kondolenzspenden

Erbitten Angehörige eine Spende an eine kirchliche Einrichtung anstelle von Blumen oder Kränzen, ist die Einrichtung für den Schutz der in diesem Zusammenhang anfallenden Spendendaten verantwortlich.

Oft treten die Angehörigen nach einiger Zeit an die bedachte Einrichtung heran und wünschen die Offenlegung der Spenderliste mit Namen und den jeweiligen Beträgen. Begründet wird der Wunsch oftmals mit dem Vorhaben, sich bei den einzelnen Spendern bedanken zu wollen.

Im Berichtsjahr gab es einige Anfragen von Einrichtungen, ob diesem Wunsch der Angehörigen nachgekommen werden darf.

Die zu den Spendern verarbeiteten Daten sind personenbezogene Daten. Eine Weitergabe der Daten darf aber nur bei Vorliegen einer rechtlichen Grundlage für die Herausgabe erfolgen.

Da zwischen den Angehörigen und den Spendern keine vertragliche Beziehung besteht, scheidet § 6 Abs. 1 lit. c KDG als Grundlage für die Weitergabe durch die Einrichtung aus. Der Spender hat seine Daten in der Regel nur zum Zweck der Erstellung einer Spendenbescheinigung für das Finanzamt gegenüber der Einrichtung angegeben.

Auch wenn der Wunsch der Angehörigen vorhanden ist, sich bei den Spendern zu bedanken, ist für die Rechtsgrundlage des berechtigten Interesses nach § 6 Abs. 1 lit. g KDG dieses Interesse der Angehörigen abzuwägen mit den Interessen der Spender. Hier wird man nicht automatisch von einem überwiegenden Interesse der Angehörigen ausgehen können, da z.B. die Spender eventuell ungenannt bleiben wollen und nicht damit rechnen mussten, dass die Daten weitergegeben werden. Auch diese Möglichkeit wird daher regelmäßig nicht als Rechtsgrundlage greifen.

Eine Einwilligung als Rechtsgrundlage für die Weitergabe der Daten an die Angehörigen wird regelmäßig daran scheitern, dass die Einwilligung informiert erfolgen muss. Der Einwilligende muss also zum Zeitpunkt der Einwilligung wissen, welchen Umfang seine Einwilligung hat. Selbst ein kurzer Hinweis in der Traueranzeige, dass die Daten der Spende an die Angehörigen weitergegeben werden, dürfte i.d.R. zu unspezifisch und nicht mit allen erforderlichen Informationen versehen sein. Auch muss eine Einwilligung aktiv und möglichst dokumentiert erfolgen.

Unproblematisch wäre auf jeden Fall, wenn der Spendenempfänger nach einiger Zeit den Angehörigen die Gesamtsumme der eingegangenen Spenden mitteilt. Die Angehörigen können die Information z.B. in einer allgemein formulierten Danksagung verwenden.

Falls die Angehörigen auf der Kenntnis der einzelnen Spender und der Beträge bestehen, wäre datenschutzrechtlich eine Möglichkeit, dass sie die Spenden selbst einsammeln (z.B. über ein auf den Namen eines Angehörigen lautendes Sonderkonto) und den Gesamtbetrag dann an die Einrichtung weiterleiten. In diesem Fall liegen die Spenderdaten direkt bei den Angehörigen und nicht bei der spendenempfangenden Einrichtung. Hierbei sind aber eventuell außerhalb des Datenschutzes liegende Folgen dieser Lösung zu beachten, wie z.B. die Frage der Ausstellung von Spendenbescheinigungen.

3.5.5 Der Brexit und die Auswirkungen auf den Datenschutz in kirchlichen Einrichtungen

Nachdem die Bürger in Großbritannien in einem Referendum 2016 für den Austritt aus der Europäischen Union (EU) gestimmt haben, soll der Austritt zum 29. März 2019 wirksam werden[15]. Bis zu diesem Zeitpunkt sollen zwischen Großbritannien und der EU Modalitäten ausgehandelt werden, wie die künftige Zusammenarbeit zu gestalten ist. Ebenso sind erforderliche rechtlich bindende Absprachen zwischen den Beteiligten zu treffen.

Von dem Ausgang der Verhandlungen zwischen Großbritannien und der EU wird abhängen, welche datenschutzrechtlichen Regelungen nach dem Austritt zur Anwendung kommen werden. Der Status Großbritanniens in Bezug auf den Datenschutz bedarf der Klärung, insbesondere hinsichtlich der Frage, ob nach einem Verlassen der EU für das Land eine den Mitgliedstaaten der EU vergleichbare Einordnung mit vergleichbaren Rechten vorgenommen wird. Von Bedeutung ist dabei auch, welche Rechtsgrundlagen gelten und welche der bisherigen Gesetze, wie etwa die DSGVO, ihre Geltung beibehalten. Denkbar wäre in diesem Zusammenhang auch, dass die Europäische Kommission zeitnah einen nach der DSGVO vorgesehenen Angemessenheitsbeschluss erlässt. Dies hätte zur Folge, dass dem Standort Großbritannien ein dem europäischen Datenschutzrecht vergleichbares Datenschutzniveau zugebilligt würde. Dadurch würde der Austausch von personenbezogenen Daten sowie die Nutzung der Angebote britischer Dienstleister im Bereich möglicher Auftragsverarbeitung erleichtert. Anderenfalls wäre Großbritannien als Drittland im Sinne der DSGVO und auch des KDG zu betrachten. In diesem Fall dürften personenbezogene Daten nur noch unter den Bedingungen eines Drittlandtransfers nach Großbritannien übermittelt werden. Gleiches würde für die Angebote britischer Firmen oder die Nutzung von britischen Speicherorten gelten.

Zum derzeitigen Zeitpunkt sind die konkreten Entwicklungen und Auswirkungen der Verhandlungen über den Brexit nicht abzusehen. Insofern kann seitens des Katholischen Datenschutzzentrums noch keine Einschätzung gegeben werden, wie sich die Ergebnisse der Beratungen und die konkrete Durchführung eines Brexits auf die Bedingungen für katholische Einrichtungen auswirken werden. Die kirchlichen Stellen sollten aber für den Fall eines ungeregelten Brexits Vorkehrungen treffen, da dann von einem Tag auf den anderen Verarbeitungen personenbezogener Daten in Großbritannien oder durch britische Dienstleister oder Wartungen von solchen Daten durch britische Dienstleister eventuell nicht mehr datenschutzkonform durchgeführt werden könnten.

15 Mittlerweile ist der Austrittstermin verschoben worden. Die Betrachtungen zu den Auswirkungen bleiben aber unverändert aktuell.

3.5.6 Cloud-Nutzung durch kirchliche Stellen

Im Berichtszeitraum gab es eine weiterhin hohe Nachfrage zu Beratungen durch das Katholische Datenschutzzentrum zu Fragen der Cloud-Nutzung durch kirchliche Einrichtungen. Hinter den Anfragen und dem Wunsch die Cloud zu nutzen standen auch im Berichtszeitraum sehr unterschiedliche Wünsche und Modelle der Cloudnutzung. Daher bleibt die Antwort auf die die Frage, was datenschutzrechtlich bei einer geplanten Cloud-Nutzung zu beachten ist, immer eine Einzelfallbetrachtung. Eine pauschale Antwort ist nicht möglich.

Wie bei er Inanspruchnahme externer Dienstleister sonst auch, sollte bei geplanten Nutzungen der Cloud ebenso darüber nachgedacht werden, was für Maßnahmen notwendig sind, wenn die Dienstleistung aus rechtlichen, tatsächlichen oder finanziellen Gründen kurz- oder mittelfristig nicht mehr (weiter)genutzt werden kann. Diese Frage wird umso wichtiger, je komplexer die Vorgänge sind, die in die Cloud ausgelagert werden sollen.

„Für die Frage der Zulässigkeit einer Cloud-Nutzung spielen neben rechtlichen Fragen auch der technisch-organisatorische Schutz der personenbezogenen Daten eine große Rolle."

Für die Frage der Zulässigkeit einer Cloud-Nutzung spielen neben rechtlichen Fragen auch der technisch-organisatorische Schutz der personenbezogenen Daten eine große Rolle.

Vor der Auslagerung der Prozesse muss die auslagernde Stelle überlegen, welche technisch-organisatorischen Schutzmaßnahmen nach § 26 KDG bisher intern gelten bzw. zukünftig vereinbart werden sollen. Mit dieser Soll-Beschreibung können die Angebote der Anbieter abgeglichen werden.

3.5.7 Veröffentlichungen der Kirchengemeinden

Im Berichtszeitraum erreichten uns mehrere Anfragen aus Kirchengemeinden, die sich auf den Umgang mit personenbezogenen Daten in den gedruckten oder anderweitig veröffentlichten Nachrichten der Gemeinde bezogen.

Die Regeln zur Veröffentlichung von kirchlichen Handlungen (Taufen, Erstkommunion, Firmung, Trauungen, Weihen und Exequien) und besonderen Ereignissen (Alters- und Ehejubiläen, Orden- und Priesterjubiläen) in Schaukasten, Pfarrbrief und Internet sind für nordrhein-westfälische (Erz-)Diözesen in den weiterhin geltenden Ausführungsrichtlinien zur KDO für den pfarramtlichen Bereich aufgeführt.

Für die Veröffentlichung in Druckwerken und Aushängen gilt die Widerspruchslösung, d.h. die Veröffentlichung ist zulässig, wenn die betroffene Person nicht vorher und rechtzeitig widersprochen hat. Auf die Möglichkeit des Widerspruchs ist regelmäßig, d.h. einmal im Jahr, hinzuweisen. Es ist aber zu beachten, dass hierbei nur Name, Vorname und Datum der kirchlichen Handlung veröffentlicht werden dürfen.

Für Veröffentlichungen auf der Homepage wird dagegen immer eine vorherige Einwilligung der betroffenen Person benötigt. Das Katholische Datenschutzzentrum empfiehlt, alle im pfarramtlichen Bereich verwendeten Anmeldeformulare so zu gestalten, dass die betroffenen Personen auf die Veröffentlichungsregeln hingewiesen werden, ihre Einwilligung zur Veröffentlichung im Internet unmissverständlich erklären oder ablehnen können und das Pfarramt die Einwilligung damit schriftlich dokumentiert hat.

Die sogenannten Intentionen, also die Messen mit besonderem Gebet z.B. für eine verstorbene Person, werden in der Ausführungsrichtlinie nicht ausdrücklich erwähnt. Da jede Messe aber eine kirchliche Handlung ist, gilt die Ausführungsrichtlinie sinngemäß.

Fraglich ist, wer als betroffene Person anzusehen ist, von dem ein Widerspruch gegen die Veröffentlichung erfolgen kann (Druckwerke) bzw. eine Einwilligung einzuholen ist (Homepage). Das Katholische Datenschutzzentrum empfiehlt, in diesen Fällen den Wünschen und Weisungen der nächsten Angehörigen zu folgen, auch wenn die Messe von einer dritten Person oder Einrichtung gestiftet wird. Die zusätzliche Nennung des Stifters ist durch eine getrennte Widerspruchs- bzw. Einwilligungslösung zu regeln.

3.5.8 Facebook-Fanpages und die gemeinsame Verantwortlichkeit für die Datenverarbeitung

In dem Urteil des Europäischen Gerichtshofs (EuGH) vom 05. Juni 2018 (Az.: C-210/16) setzt sich das Gericht mit der Frage auseinander, wer bei einer Facebook-Fanpage als Verantwortlicher im Sinne des Datenschutzes herangezogen werden kann.

In der dem EuGH durch das Bundesverwaltungsgericht vorgelegten Frage der Auslegung der Richtlinie 95/46/EG geht es inhaltlich darum, ob im Fall des Verstoßes gegen datenschutzrechtliche Bestimmungen, gegen den Betreiber der Fanpage vorgegangen werden kann oder gegen Facebook bzw. die irische Tochtergesellschaft Facebook Ireland (für die Europäische Union) (in dem konkreten Fall ging es um Informationspflichten, dass Facebook mittels Cookies personenbezogene Daten der Fanpage-Besucher sammelt und weiterverarbeitet). Auch wenn die Entscheidung des EuGH noch zur Datenschutz-Richtlinie aus 1995 erging, die Grundlage für das bis Mai 2018 geltende Datenschutzrecht war, sind die Ausführungen zur Verantwortlichkeit auch auf die neue Rechtslage nach der Datenschutz-Grundverordnung bzw. dem Kirchlichen Datenschutzgesetz übertragbar.

Unproblematisch stellt der EuGH in seinem Urteil zunächst klar, dass Facebook/Facebook Ireland als Verantwortlicher im Sinne der Datenschutzgesetze anzusehen ist, da diese über die Verarbeitung personenbezogener Daten bei der Nutzung von Facebookseiten entscheiden. Relevant ist jedoch, dass in dem Urteil festgestellt wird,

dass der Betreiber der Facebookseite, das heißt derjenige oder die Einrichtung, welche auf der Facebookseite dargestellt ist und diese eingerichtet hat, als gemeinsam mit Facebook/Facebook Ireland verantwortlich angesehen wird, da dieser auch durch verschiedene Steuerungsmöglichkeiten (insbesondere demografische und geografische Daten) in Verbindung mit der Fanpage über die Zwecke und Mittel der Verarbeitung personenbezogener Daten (mit-)entscheidet. Dabei liegt die Betonung des Urteils darauf, dass der Schutz der personenbezogenen Daten der Besucher einer Facebook-Fanpage durch die gemeinsame Verantwortlichkeit erhöht wird.

Der EuGH hat im Rahmen eines Vorabbeschlussverfahrens über diese Rechtsfrage entschieden. Die nationale Streitigkeit ist dadurch nicht entschieden, jedoch muss das nationale Gericht in Einklang mit dieser Entscheidung urteilen.

Aus dem Urteil ergibt sich, dass Betreiber einer Facebook-Fanpage somit für die personenbezogenen Daten der Besucher der Seite gemeinsam mit Facebook verantwortlich sind und damit entsprechende Informationspflichten haben und diesen nachkommen müssen. Somit muss der Grundsatz der Transparenz insofern eingehalten werden, dass die Besucher einer Facebook-Fanpage (registriert oder nicht) darüber informiert werden, welche Daten zu welchen Zwecken durch den Betreiber der Fanpage oder Facebook verarbeitet werden. Werden Daten durch Tracking (zB. Cookies oder Speichern der IP-Adresse) weiterverarbeitet, bedarf dies regelmäßig der Einwilligung der Besucher der Fanpage. Daher muss sichergestellt sein, dass der Betreiber einer solchen Fanpage selbst durch Facebook darüber informiert ist, welche personenbezogenen Daten der Besucher auf welche Weise verarbeitet werden (unter anderem auch um die Betroffenenrechte gewährleisten zu können). Dies erfordert jedoch die Zusammenarbeit mit Facebook. Facebook muss somit ein den datenschutzrechtlichen Bestimmungen angepasstes Produkt anbieten, damit die Betroffenenrechte gewahrt werden und ein datenschutzkonformer Betrieb in Europa möglich ist.

Da auch viele kirchliche Einrichtungen sogenannte Fanpages betreiben, weist die Konferenz der Diözesandatenschutzbeauftragten mit Beschluss vom 26.07.2018 darauf hin, dass ein datenschutzrechtlich konformer Betrieb einer Fanpage zum jetzigen Zeitpunkt als bedenklich eingestuft wird, solange keine ausreichenden Vereinbarungen mit Facebook getroffen werden (können).

3.5.9 Neue Techniken auf Webseiten - neue Datenschutzprobleme? Web-Push-Benachrichtigungen und der Einsatz des Facebook-SDK

Web-Push-Benachrichtigungen

Wer sich über Neuigkeiten eines Unternehmens, einer Behörde oder aus einer sonstigen Quelle regelmäßig und ohne eigenes Nachfragen informieren möchte, hat schon seit längerer Zeit die Möglichkeit, einen „Newsletter" zu abonnieren. Auch das Katholische Datenschutzzentrum bietet diese Möglichkeit.

Das Abonnieren des Newsletters stellt datenschutzrechtlich eine Einwilligung in die jederzeitige Kontaktaufnahme per E-Mail-Newsletter dar und unterliegt deshalb den bekannten Vorschriften. Beispielsweise muss die Einwilligung informiert und freiwillig erfolgen, weshalb die Anbieter i.d.R. eine Bestätigung des Abonnements durch Antwort auf eine initiale Mail verlangen (Double-Opt-In). Das Abbestellen muss ebenso einfach organisiert sein. Die Anbieter schicken deshalb i.d.R. mit jedem Newsletter einen Link, über den die Abbestellung vorgenommen werden kann.

Das Medium E-Mail ist allerdings in den Augen vieler Nutzer und Informationsanbieter nicht mehr zeitgemäß. Vielmehr werden Informationen in schneller Sequenz, ähnlich wie bei Push-Nachrichten in Messengern und anderen Anwendungen auf mobilen Endgeräten erwartet. Um diese Form der Informationsübermittlung auch im Umfeld von Desktop-Browsern zu realisieren, steht seit einiger Zeit die Technik der Web-Push-Nachrichten zur Verfügung.

Der Anbieter fragt den Nutzer zu einem bestimmten Zeitpunkt, etwa beim erstmaligen Aufrufen der Homepage, nach der Einwilligung, in den Verteiler der Push-Nachrichten aufgenommen zu werden. Die Information, ob die Einwilligung erteilt wurde, wird vom Anbieter gespeichert und gleichzeitig im Browser des Anwenders abgelegt. Auch eine Ablehnung der Push-Nachrichten wird im Browser gespeichert. Ab der Einwilligung erhält der Nutzer Push-Nachrichten in einer vom Anbieter festgelegten Frequenz. Voraussetzung ist lediglich der gestartete Browser. Die Push-Nachricht wird angezeigt unabhängig davon, ob der Nutzer gerade auf der Website des Anbieters ist oder irgendeine andere Seite anzeigt.

Datenschutzrechtlich problematisch ist die oft nicht offensichtliche Möglichkeit der Abbestellung, also des Widerrufens der Einwilligung. Hierzu muss nämlich der Nutzer in die Einstellungen des Browsers wechseln und dort nach mehreren Klicks durch das Einstellungsmenü unter den erteilten Berechtigungen diejenige suchen und löschen, die der Website des fraglichen Anbieters zur Sendung der Push-Nachrichten erteilt wurde. Der Widerruf der Einwilligung muss also i.d.R. auf

einem anderen Weg erfolgen als die Einwilligung zuvor erfolgte. Hier ist teilweise noch nachzubessern, damit der Widerruf wirklich „so einfach wie die Erteilung der Einwilligung" vorgenommen werden kann (§ 8 Abs. 6 Satz 4 KDG).

Verwendung des Facebook-Software-Development-Kit

Wenn sich katholische Einrichtungen (z.B. Kirchengemeinden oder Vereine) oder Gruppen innerhalb dieser Einrichtungen (z.B. Messdiener- oder Jugendgruppen) entschließen, eine eigene mobile App zur Kommunikation und zur Verteilung spezifischer Informationen innerhalb der Gruppe zu erstellen, wird oft auf das kostenlose Angebot des Facebook-Software-Development-Kit zurückgegriffen.

Dieses Entwicklungswerkzeug bringt viele Funktionen mit, die den Zweck der App unterstützen und deshalb von den oft ehrenamtlichen Entwicklern der App nicht mehr selbst programmiert werden müssen, wie z.B. die Anmeldung über den Facebook-Account oder eine sonstige Identifizierung (per E-Mail, Telefonnummer), das Teilen von Inhalten, Verknüpfungen zum Facebook-Messenger oder einen Kalender.

Problematisch ist hier, dass das Entwicklungswerkzeug von Facebook eine Reihe von Tracking- und Protokollierungsfunktionen mitbringt, die vom Nutzer – zumindest zum Start einer mit dem Facebook-Software-Development-Kit gebauten App – nicht beeinflussbar oder abschaltbar sind. Viele so gebaute Apps nehmen nach dem Start zuerst einmal Kontakt mit den Facebook-Servern auf und übermitteln eine Reihe von Statusinformationen, bevor der Anwender die Chance bekommt, der Übermittlung seiner Daten zu widersprechen. Nur der Entwickler kann das Verhalten der App beim Programmstart festlegen, macht sich aber meistens keine Gedanken, die nicht datenschutzkonformen Voreinstellungen des Entwicklungswerkzeuges abzuändern.

Das Katholische Datenschutzzentrum hat im Berichtsjahr eine Testumgebung aufgebaut, in der Android-Apps installiert und bezüglich ihres offenen oder verdeckten Kommunikationsverhaltens analysiert werden können. In Zukunft sollen vermehrt Applikationen, die von kirchlichen Einrichtungen genutzt oder selbst entwickelt wurden, auf die Einhaltung des Datenminimierungsprinzips und der verpflichtenden Einholung von Einwilligungen zur Datenübertragung überprüft werden.

3.5.10 Messengerdienste (insbesondere WhatsApp)

Die datenschutzkonforme dienstliche Nutzung von Messengerdiensten ist auch in diesem Berichtszeitraum eines der am häufigsten angefragten Themen gewesen.

Auch wenn WhatsApp im privaten Bereich der am weitesten verbreitete Messenger sein mag, so haben der Bundesdatenschutzbeauftragte, die Landesdatenschutzbeauftragten und die Datenschutzaufsichten der Evangelischen und der Katholischen Kirche bis jetzt immer wieder feststellen müssen, dass die fehlende umfassende Beachtung der europäischen datenschutzrechtlichen Regelungen bzw. der kirchlichen Regelungen (KDG oder DSG-EKD) es den Verantwortlichen unmöglich macht, diesen Dienst in der Standardvariante für die dienstliche Kommunikation einzusetzen.

Die Diözesandatenschutzbeauftragten sind nicht grundsätzlich gegen den Einsatz von Messengern. Sie haben Kriterien veröffentlicht, wie aus den am Markt befindlichen Diensten ein datenschutzkonformer Dienst ausgewählt werden kann[16].

Nicht die Kommunikationsform an sich ist das Problem, sondern dass einzelne Messenger die europäischen und damit auch kirchlichen Vorgaben in Sachen Datenschutz nicht vollumfänglich einhalten.

Bei WhatsApp stellt sich weiterhin das Problem, dass das Telefonbuch des Nutzers ungefragt ausgelesen und an WhatsApp/Facebook übermittelt wird. Da für diese Datenübermittlung an einen Dritten, nämlich von der kirchlichen Stelle an WhatsApp, in der Regel keine Rechtsgrundlage vorhanden sein wird, verstößt die kirchliche Stelle als Verantwortlicher im Sinne des KDG gegen den Datenschutz.

Ebenfalls problematisch ist die Datensammlung des Unternehmens über die Nutzungsgewohnheiten der Kunden. Auch wenn durch eine Ende-zu-Ende Verschlüsslung die Inhaltsdaten der Kommunikation wohl für WhatsApp nicht verwendbar sind, stehen WhatsApp die Metadaten der Kommunikation zur Verfügung. Über diese lassen sich genaue Nutzungsprofile erstellen.

Es besteht daher für alle kirchlichen Organisationen Handlungsbedarf. Einzelne (Erz-)Diözesen haben den Einsatz von WhatsApp schon völlig untersagt[17].

„Es besteht (...) für alle kirchlichen Organisationen Handlungsbedarf. Einzelne (Erz-)Diözesen haben den Einsatz von WhatsApp schon völlig untersagt."

16 Siehe Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 26.07.2018 zur Beurteilung von Messenger- und Social-Media-Diensten; Beschluss abgedruckt in Kapitel 6 dieses Berichtes.

17 So z.B. das Erzbistum Berlin (siehe https://www.erzbistumberlin.de/medien/kdg-faq/ Stichwort WhatsApp); abgerufen am 12.04.2019.

3.5.11 Einwilligungen

Nach § 6 Abs. 1 lit. b) KDG ist die Einwilligung eine der möglichen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Die Voraussetzungen für eine wirksame Einwilligung sind in § 8 KDG näher beschrieben. An eine solche Einwilligung sind jedoch strenge Anforderungen zu stellen. Sind diese nicht erfüllt, liegt keine wirksame Einwilligung vor.

Die schon im letzten Jahresbericht erläuterten Voraussetzungen für eine wirksame Einwilligung nach KDO[18] haben sich unter der Geltung des neuen KDG nicht verändert. Es bedarf immer noch einer informierten, freiwilligen und in der Regel schriftlichen Willensäußerung der einwilligenden Person.

Um eine wirksame Einwilligung erteilen zu können bedarf es nicht der zivilrechtlichen Geschäftsfähigkeit, sondern es reicht die Urteils- und Einsichtsfähigkeit der betroffenen Person in die Auswirkungen und die Reichweite der Einwilligung aus.

Generelle, abstrakte Erklärungen sind nicht präzise genug, um die Verarbeitung personenbezogener und damit besonders zu schützender Daten zu erlauben. Das bedeutet, dass die betroffene Person über Art und Umfang der Einwilligung umfassend in Kenntnis gesetzt werden muss und gegebenenfalls bestehende Aufklärungspflichten einzuhalten sind. Weiterhin muss die betroffene Person über die Möglichkeit des Widerrufs seiner erteilten Einwilligung für die Zukunft informiert werden.

Gerade vor dem Hintergrund der Widerrufbarkeit der Einwilligung ist es für die Verantwortlichen meist günstiger, sich auf eine evtl. bestehende andere Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten zu stützen.

18 Siehe Jahresbericht 2017, Abschnitt 3.3.8 auf Seite 34.

3.6 Meldepflicht der Verletzung des Schutzes personenbezogener Daten gemäß § 33 KDG

§ 33 KDG gibt den Verantwortlichen im Sinne des KDG vor, dass der Verantwortliche der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten zu melden hat, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. Eine vergleichbare Norm fand sich in der Anordnung über den kirchlichen Datenschutz (KDO) vor Inkrafttreten des KDG nicht. In der alten Fassung des Bundesdatenschutzgesetzes hingegen bestand eine - wenn auch nicht ganz so umfangreiche - Meldeverpflichtung in § 42a BDSG a.F..

Parallel zu der Regelung in der DSGVO enthält auch die Meldepflicht nach § 33 KDG - anders als § 42 BDSG a.F. - keine Beschränkungen in dem Sinne, dass eine Meldepflicht nur bei bestimmten Datenarten besteht.

Daher ist dies für die kirchlichen Einrichtungen eine neue gesetzliche Verpflichtung, welche zum Schutz der personenbezogenen Daten dienen und besonders die Verarbeitungsprozesse mit den technischen und organisatorischen Schutzmaßnahmen verbessern soll, um wiederholte Verletzungen des Schutzes personenbezogener Daten möglichst zu vermeiden. Korrespondierend zu dieser neuen Regelung ist auch die Regelung in § 34 KDG neu für die Einrichtungen. Diese besagt, dass die von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen durch den Verantwortlichen zu benachrichtigen sind, wenn voraussichtlich ein hohes Risiko für deren persönliche Rechte und Freiheiten besteht. Dies setzt voraus, dass der Verantwortliche eine Risikoabwägung vornimmt, welche das bestehende Risiko bewertet.

Das Katholische Datenschutzzentrum richtete - zusammen mit den anderen Diözesandatenschutzbeauftragten – eine elektronische Möglichkeit ein, über die die Meldungen, die innerhalb von 72 Stunden nach Bekanntwerden der Datenschutzverletzung abzugeben sind, über die Internetseiten der Datenschutzaufsichten abgegeben werden können.

Das Katholische Datenschutzzentrum erhielt im Berichtszeitraum unter der Geltung des neuen Gesetzes von Ende Mai bis Jahresende deutlich mehr Datenschutzverletzungen gemeldet, als es unter der alten Rechtslage als Beratungs- oder Prüfvorgänge zur Kenntnis bekommen hat.

Nach einer ersten Einschätzung hat sich das Instrument der Meldung dieser Vorgänge bewährt, um mit den kirchlichen Einrichtungen zusammen sicherzustellen, dass sich die Vorgänge nicht wiederholen, die zur Verletzung der Rechte und Freiheiten der betroffenen Personen geführt haben.

3.7 Bußgelder

„Im Berichtszeitraum hat das Katholische Datenschutzzentrum noch keine Geldbuße verhängt."

Das seit Ende Mai 2018 geltende Kirchliche Datenschutzgesetz sieht in § 51 KDG jetzt auch vor, dass die Datenschutzaufsicht gegen einen Verantwortlichen oder einen Auftragsverarbeiter eine Geldbuße verhängen kann, wenn dieser vorsätzlich oder fahrlässig gegen Bestimmungen des KDG verstößt. Dabei soll die Geldbuße gemäß § 51 Abs. 2 KDG „für Verstöße gegen dieses Gesetz in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein, wobei § 51 Abs. 5 KDG den Höchstbetrag für eine Geldbuße auf 500.000 Euro festlegt hat.

Im Berichtszeitraum hat das Katholische Datenschutzzentrum noch keine Geldbuße verhängt.

3.8 Verfahren vor dem kirchlichen Datenschutzgericht

Da die Befugnisse der Datenschutzaufsicht mit dem KDG erheblich erweitert wurden und neben Eingriffsbefugnissen in die Datenverarbeitung der Verantwortlichen auch die Möglichkeit der Verhängung von Bußgeldern erstmals gegen kirchliche Stellen möglich ist, war es notwendig, wirksame gerichtliche Rechtsbehelfe gegen die Maßnahmen der Datenschutzaufsicht sicherzustellen.

Das KDG sieht in § 49 KDG eine gerichtliche Überprüfung der Entscheidungen der Aufsicht vor. Zu diesem Zweck hat die Katholische Kirche mit der Kirchlichen Datenschutzgerichtsordnung (KDSGO) ein Gerichtsgesetz geschaffen und damit eigene Datenschutzgerichte, das Interdiözesane Datenschutzgericht als erste Instanz und das Datenschutzgericht der Deutschen Bischofskonferenz als zweite Instanz, eingerichtet.

Im Berichtszeitraum wurde kein Rechtsbehelf gegen Entscheidungen des Katholischen Datenschutzzentrums eingelegt.

4 Das Katholische Datenschutzzentrum

4.1 Zuständigkeitsbereich

Der Diözesandatenschutzbeauftragte als Leiter des Katholischen Datenschutzzentrums ist als Datenschutzaufsicht im Sinne des Art. 91 Abs. 2 DSGVO und der §§ 42 ff. KDG für die fünf nordrhein-westfälischen (Erz-)Diözesen zuständig. Diese sind von der Fläche deckungsgleich mit dem Bundesland Nordrhein-Westfalen. Hinzu kommen noch einzelne Gemeinden oder Teile von Gemeinden in Rheinland-Pfalz, die zur Erzdiözese Köln gehören, und in Niedersachsen und in Hessen, die zur Erzdiözese Paderborn gehören. In diesem Gebiet leben über 6,9 Millionen Menschen römisch-katholischen Glaubens (Stand 2017).

Neben den fünf (Erz-)Bischöflichen Generalvikariaten als den zentralen Verwaltungsbehörden der (Erz-)Diözesen werden die vielen Pfarreien vor Ort vom Katholischen Datenschutzzentrum betreut. Hinzu kommen fünf Caritasverbände auf Diözesanebene und ca. 80 örtliche Verbände der Caritas mit ihren Beratungsangeboten und Beratungsstellen (Stand 2015). Daneben gibt es in den fünf (Erz-) Diözesen noch über 140 Schulen in kirchlicher Trägerschaft, über 2600 katholische Kindergärten, rund 200 katholische Krankenhäuser, über 640 Altenpflegeeinrichtungen und rund 390 Einrichtungen der Jugendhilfe für die der Diözesandatenschutzbeauftragte zuständig ist (Stand 2013). Darüber hinaus fallen noch diverse Vereine, Verbände und Stiftungen im kirchlichen Bereich in die Zuständigkeit des Diözesandatenschutzbeauftragten. Auch die Bundesverbände kirchlicher Vereinigungen, die ihren Sitz in Nordrhein-Westfalen haben, fallen auf Grund ihres Sitzes in die Zuständigkeit des Katholischen Datenschutzzentrums.

Seit dem 01.01.2018 ist der Diözesandatenschutzbeauftragte zusätzlich als Datenschutzaufsicht für den Verband der Diözesen Deutschlands (VDD) zuständig. Der VDD ist Rechtsträger der Deutschen Bischofskonferenz. Er wurde 1968 als Körperschaft des öffentlichen Rechts gegründet. Im VDD sind die 27 rechtlich und wirtschaftlich selbstständigen Diözesen zusammengeschlossen. Neben dem Sekretariat der Deutschen Bischofskonferenz in Bonn gehören unter anderem die Geschäftsstelle des VDD in Bonn, das Kommissariat der deutschen Bischöfe – Katholisches Büro in Berlin und weitere Einrichtungen des VDD zum Zuständigkeitsbereich.

4.2 Aufbau der Einrichtung

Das Katholische Datenschutzzentrum ist eine eigenständige Körperschaft des öffentlichen Rechts. Die Körperschaft des öffentlichen Rechts wurde gegründet von den Erzdiözesen Köln und Paderborn und den Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil).

In den Verwaltungsrat des Katholischen Datenschutzzentrums haben die (Erz-)Bischöfe ihre jeweiligen Generalvikare entsandt. Der Vertreter der Erzdiözese Paderborn, Herr Generalvikar Hardt, wurde vom Verwaltungsrat zum Vorsitzenden des Gremiums gewählt. Die Geschäftsführung des Gremiums wurde dem Leiter des Katholischen Datenschutzzentrums übertragen.

Die Leitung des Katholischen Datenschutzzentrums nimmt der gemeinsame Diözesandatenschutzbeauftragte der fünf Mitgliedsdiözesen des Katholischen Datenschutzzentrums wahr. Er vertritt die Körperschaft nach außen.

Dem Diözesandatenschutzbeauftragten sind ein Vertreter, Referenten, Sachbearbeiter und Sekretariatskräfte zur Seite gestellt, die auch vom Katholischen Datenschutzzentrum selbst angestellt sind. Von den elf Stellen sind zum Jahresende zehn besetzt.

Durch die eigenständige Körperschaft des öffentlichen Rechts und das im eigenen Haus angestellte Personal wird die notwendige Unabhängigkeit des Diözesandatenschutzbeauftragten und seiner Mitarbeiter gewährleistet.

	Soll	Ist
DDSB / VDSB/ Leiter KDSZ	1	1
Stv. DDSB / stv. VDSB / stv. Leiter KDSZ	1	1
Referentinnen / Referenten	5	4
Sachbearbeiterinnen / Sachbearbeiter	2	2
Sekretariat	2	1,77
Gesamt	11	9,77

Personalausstattung KDSZ zum 31.12.2018 (in Vollzeitstellen)

Bei der Planung des Katholischen Datenschutzzentrums wurde konsequent auf die Umsetzung des Urteils des Europäischen Gerichtshofes vom 09.03.2010 zur Unabhängigkeit und Selbständigkeit der Datenschutzaufsichtsbehörden[19] geachtet und die Veränderungen durch die Europäische Datenschutz-Grundverordnung bzw. deren Umsetzung in kirchliches Recht schon berücksichtigt.

Das Katholische Datenschutzzentrum hat seinen Sitz im Hause des Sozialinstituts der Kommende Dortmund, einer Einrichtung der Erzdiözese Paderborn.

Im April 2018 konnte das Katholische Datenschutzzentrum seine neuen Büroräume in der umgebauten zweiten Etage der Kommende beziehen. In der gut neunmonatigen Umbauzeit hat das Erzbistum Paderborn hier moderne Arbeitsbedingungen für das Katholische Datenschutzzentrum geschaffen. Am 14.06.2018 wurden die neuen Büroräume im Rahmen einer kleinen Feierstunde vom Vorsitzenden des Verwaltungsrates des Katholischen Datenschutzzentrums und Generalvikar des Erzbistums Paderborn Herrn Generalvikar Alfons Hardt eingesegnet.

Nach der Übernahme der Aufgaben des Diözesandatenschutzbeauftragten der fünf (Erz-)Diözesen in NRW zum 01.09.2016 und dem Aufbau der Einrichtung im Jahr 2017 nahm im Berichtszeitraum die Vorbereitung auf das neue Datenschutzgesetz, das nicht nur für die kirchlichen Einrichtungen, sondern auch für das Katholische Datenschutzzentrum Handlungsbedarf auslöste, und die Beratung der kirchlichen Einrichtungen zu den neuen Regelungen den größten Anteil der Arbeit ein.

Mit der Übernahme der Datenschutzaufsicht über den VDD und die angeschlossenen Einrichtungen wurde diese Aufgabe in die bestehenden Abläufe des Katholischen Datenschutzzentrums integriert und so die reibungslose Wahrnehmung der Datenschutzaufsicht auch für diese kirchlichen Stellen sichergestellt.

19 Siehe hierzu schon oben Kap. 2.1.

4.3 Finanzen

Das Katholische Datenschutzzentrum wird von den fünf (Erz-)Diözesen als Mitglieder der Körperschaft des öffentlichen Rechts getragen. Wie in § 17 Abs. 3 KDO bzw. § 43 Abs. 4 KDG beschrieben, stellen sie die für die Erfüllung der Aufgaben des Diözesandatenschutzbeauftragten angemessene Personal- und Sachausstattung zur Verfügung. Außerdem verfügt der Diözesandatenschutzbeauftragte über einen eigenen jährlichen Haushalt.

Für das Kalenderjahr 2018 hat der Verwaltungsrat des Katholischen Datenschutzzentrums auf Vorschlag des Diözesandatenschutzbeauftragten den Haushaltsplan in Höhe von 1.334.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben bewilligt.

Für das Folgejahr 2019 wird sich das genehmigte Budget auf Grund von zusätzlichen Ausgaben für die Umsetzung der neuen gesetzlichen Regelungen auf 1.400.000 Euro erhöhen.

4.4 Vertretung in Gremien und Arbeitsgruppen in der Katholischen Kirche

Das Katholische Datenschutzzentrum ist weiterhin mit einem Referenten in der Unterarbeitsgruppe der Ständigen Arbeitsgruppe Datenschutz- und Melderecht/IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands (VDD) vertreten. Diese Unterarbeitsgruppe hat sich nach der Erstellung des Vorschlags für das neue kirchliche Datenschutzgesetz im Jahr 2018 schwerpunktmäßig mit der Neufassung der Durchführungsverordnung zum neuen Datenschutzgesetz beschäftigt, die zum 01. März 2019 in den (Erz-)Diözesen in Kraft gesetzt werden soll.

Bei der Weiterentwicklung der diözesanen Gesetze und der Diskussion von grundsätzlichen Rechtsfragen sind die Justitiarinnen und Justitiare der fünf (Erz-)Diözesen und der Justitiar des Katholischen Büros NRW in Düsseldorf die ersten Ansprechpartner des Katholischen Datenschutzzentrums.

Das Katholische Datenschutzzentrum hält daher einen regelmäßigen Kontakt zu den Rechtsabteilungen der Generalvikariate und zum Katholischen Büro NRW.

4.5 Vernetzung

4.5.1 Vernetzung mit kirchlichen Stellen

Die fünf Diözesandatenschutzbeauftragten der deutschen (Erz-) Diözesen stehen in ständigem Austausch untereinander und mit den beiden gemeinsamen Ordensdatenschutzbeauftragten der Deutschen Ordensobernkonferenz zu aktuellen Fragen und grundsätzlichen Themen. Die Besprechungen und Telefon- oder Videokonferenzen dienen diesem Austausch und der Vorbereitung und Verabschiedung gemeinsamer Beschlüsse[20].

Der Beauftragte für den Datenschutz der EKD (BfD EKD) hat neben seinem Hauptsitz in Hannover noch vier Außenstellen. Die Außenstelle in Dortmund ist u.a. für die Landeskirchen und Diakonien in NRW zuständig. Mit der Außenstelle Dortmund des BfD EKD ist im Berichtszeitraum der regelmäßige Austausch fortgesetzt worden.

Außerdem unterstützt das Katholische Datenschutzzentrum im Rahmen seiner zeitlichen Möglichkeiten Arbeitskreise betrieblicher Datenschutzbeauftragter kirchlicher Einrichtungen. Hierbei steht das Katholische Datenschutzzentrum für kurze Vorträge und allgemeinen Erfahrungsaustausch zur Verfügung.

So hat das Katholische Datenschutzzentrum mit den betrieblichen Datenschutzbeauftragten der Generalvikariate, den IT-Sicherheitsbeauftragten der (Erz-)Diözesen oder den IT-Verantwortlichen der Generalvikariate verschiedene Gesprächskreise aufgebaut, die dem regelmäßigen Austausch dienen.

„Außerdem unterstützt das Katholische Datenschutzzentrum (...) Arbeitskreise betrieblicher Datenschutzbeauftragter kirchlicher Einrichtungen."

4.5.2 Vernetzung mit staatlichen Stellen

Der Kontakt und der Austausch mit der Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten als staatlichen Datenschutzaufsichtsbehörden ist nach § 18 Abs. 5 KDO bzw. § 46 KDG Bestandteil der Aufgaben des Diözesandatenschutzbeauftragten. Im Berichtszeitraum gab es vielfältige regelmäßige Kontakte in Grundsatzfragen und bei der Bearbeitung von konkreten Datenschutzproblemen.

Diese Kontakte zu den staatlichen Stellen helfen, vergleichbare Auslegungen der Gesetze bei vergleichbaren Vorgängen und damit ein vergleichbares Datenschutzniveau sicherzustellen.

§ 18 Abs. 1 Satz 4 Bundesdatenschutzgesetz (BDSG) sieht eine Beteiligung der kirchlichen Datenschutzaufsichten bei bestimmten Sachverhalten vor, die vom Europäischen Datenschutzausschuss beraten werden, wenn die kirchlichen Datenschutzaufsichten von dieser

20 Siehe Kapitel 2.2 dieses Berichtes zur Konferenz der Diözesandatenschutzbeauftragten und Kapitel 6 dieses Tätigkeitsberichtes zu den Beschlüssen der Konferenz.

Frage betroffen sind. Die Einzelheiten zur Anwendung dieser Vorschrift sind zwischen den staatlichen Datenschutzaufsichten und den Datenschutzaufsichten der Rundfunkanstalten und der Kirchen noch in der Diskussion.

In seiner Funktion als Leiter des Arbeitskreises Technik der Konferenz der Diözesandatenschutzbeauftragten nimmt der stellv. Leiter des Katholischen Datenschutzzentrums auch an dem Arbeitskreis Technik der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder teil.

4.6 Öffentlichkeitsarbeit

Das Katholische Datenschutzzentrum macht auf vielfältige Weise auf den Datenschutz in der Katholischen Kirche und seine Arbeit aufmerksam und informiert die kirchlichen Einrichtungen, die betroffenen Personen und die interessierte Öffentlichkeit über den Datenschutz in der Katholischen Kirche.

Die Bedeutung der Informationsweitergabe und der Öffentlichkeitsarbeit wird durch das neue Gesetz besonders herausgestellt. So ist im Aufgabenkatalog der Datenschutzaufsichten in § 44 Abs. 3 KDG dieses Thema gleich mehrfach betont.

So sollen die Datenschutzaufsichten gemäß § 44 Abs. 3 lit. a) KDG die „Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären", wobei „spezifische Maßnahmen für Minderjährige" besondere Beachtung finden sollen. Weiterhin sollen die Datenschutzaufsichten „kirchliche Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten" (§ 44 Abs. 3 lit. b) KDG), „die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz entstehenden Pflichten sensibilisieren" (§ 44 Abs. 3 lit. c) KDG) und „auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes zur Verfügung stellen" (§ 44 Abs. 3 lit. d) KDG).

4.6.1 Internetauftritt

Über die Internetpräsenz www.katholisches-datenschutzzentrum.de stellt das Katholische Datenschutzzentrum vielfältige Informationen rund um den kirchlichen Datenschutz und die Arbeit der Datenschutzaufsicht zur Verfügung. Diese Informationen sind als Internetseiten online verfügbar oder stehen dort als Infoblätter / Broschüren zum Download bereit. Hierbei reicht das Spektrum von den einschlägigen Gesetzestexten für die jeweilige (Erz-)Diözese über Hilfestellungen bis hin zu Mustern.

Viel Wert wurde unter anderem auf die Sicherheit gelegt, was z. B. auch ein gesichertes Kontaktformular beinhaltet. Über diese Kontaktmöglichkeit will das Katholische Datenschutzzentrum jedem Beteiligten eine gesicherte Kontaktaufnahme ermöglichen.

Das Katholische Datenschutzzentrum verschickt auch einen Newsletter, der regelmäßig über neue Informationen auf der Internetseite informiert. Der Newsletter kann über die Internetseite abonniert werden.

4.6.2 Vorträge

Wie schon im zweiten Halbjahr 2017 war auch im Jahr 2018 die Nachfrage nach Vorträgen durch das Katholische Datenschutzzentrum ungebrochen hoch. Nachdem die Termine rund um das Inkrafttreten des neuen Datenschutzgesetzes Ende Mai 2018 sehr hoch waren, schwächte sich die Nachfrage im zweiten Halbjahr leicht ab, blieb aber weiterhin auf einem hohen Niveau. Wie in den Vorjahren waren dabei verschiedenste Gruppen und Formate vertreten. Bei diesen Informationsveranstaltungen ist das Katholische Datenschutzzentrum als Referent vertreten, organisiert die Veranstaltungen aber nicht selbst.

Mit diesen Vorträgen konnten wieder hunderte Multiplikatoren und Verantwortliche erreicht werden.

Auch wenn Fragen zum neuen Datenschutzgesetz im Vordergrund standen, war der Informationsbedarf der kirchlichen Stellen, der betroffenen Personen und der Öffentlichkeit zum kirchlichen Datenschutz im Allgemeinen im Berichtszeitraum weiterhin unvermindert hoch.

4.6.3 Informationen/Broschüren/Arbeitshilfen/Muster

Neben den Informationen auf der Internetseite stellt das Katholische Datenschutzzentrum auch noch weitergehende Informationen in Form von Informationsblättern, Broschüren, Arbeitshilfen, Mustern oder Checklisten bereit.

So wurden im Berichtszeitraum z.B. ein Informationsblatt zum Ablauf von Prüfungen durch das Katholische Datenschutzzentrum und ein aktualisiertes Informationsblatt zum erweiterten Führungszeugnis bereitgestellt. Zum Thema Verzeichnis der Verarbeitungstätigkeiten erstellte das Katholische Datenschutzzentrum eine Formulierungshilfe und mit der Konferenz der Diözesandatenschutzbeauftragten zusammen eine Formulierungshilfe zu den Informationspflichten nach dem KDG oder der Weitergeltung der KDO-DVO unter dem neuen KDG.

Die zusammen mit den anderen Diözesandatenschutzbeauftragten gemeinsam verfasste Schriftenreihe (Praxishilfen) zum neuen kirchlichen Gesetz für den Datenschutz wurde weitergeführt und aktualisiert.

4.6.4 Das Katholische Datenschutzzentrum auf dem 101. Katholikentag in Münster

Das Katholische Datenschutzzentrum hat aktiv am 101. Katholikentag Anfang Mai in Münster teilgenommen und sich und seine Arbeit auf der Kirchenmeile präsentiert sowie eine Podiumsdiskussion veranstaltet.

An den drei Tagen, in denen die Kirchenmeile geöffnet hatte, stand das Katholische Datenschutzzentrum zu seiner Arbeit und zu Fragen rund um den (neuen) Datenschutz Rede und Antwort. Unterstützt wurde das Katholische Datenschutzzentrum dabei auch von Kolleginnen und Kollegen der anderen Datenschutzaufsichten der Katholischen Kirche in Deutschland. Der Stand war durchgängig gut besucht. Im Rahmen der Gespräche konnten viele Fragen beantwortet, Hinweise zur Umsetzung des Datenschutzes gegeben und über die Arbeit des Hauses berichtet werden.

„Im Rahmen der Gespräche konnten viele Fragen beantwortet, Hinweise zur Umsetzung des Datenschutzes gegeben und über die Arbeit (des Katholischen Datenschutzzentrums) berichtet werden."

Da das Inkrafttreten des Gesetzes über den Kirchlichen Datenschutz am 24. Mai zu diesem Zeitpunkt kurz bevorstand, gab es einen hohen Beratungsbedarf in datenschutzrechtlichen Fragestellungen.

Daneben veranstaltete das Katholischen Datenschutzzentrum im Rahmen der Vorträge beim Katholikentag eine Podiumsdiskussion zum Thema „Bleiben Sie Herr Ihrer Daten!". Als Teilnehmer der Diskussion nahmen Herr Prof. Dr. Hoeren von der Westfälischen Wilhelms-Universität in Münster, Frau Dr. Kurz vom Chaos Computer Club, Herr Dr. Kleffner aus der Diözese Essen und Herr Steffen Pau als Diözesandatenschutzbeauftragter und Leiter des Katholischen Datenschutzzentrums teil. Das Interesse an der Podiumsdiskussion als Besucher teilzunehmen war so groß, dass die Raumgröße und damit die vorhandenen Sitzplätze nicht ausreichten. Es kam zu einer anregenden Diskussion, welche unter anderem technische Themen aus datenschutzrechtlicher Sitz kritisch beleuchtete, aber auch Probleme der Praxis in Kirchengemeinden und Vereinen wurden thematisiert.

Nach dem Abschlussgottesdienst konnten die Kolleginnen und Kollegen des Katholischen Datenschutzzentrums eine rundum positive Bilanz der aktiven Beteiligung der Datenschutzaufsicht am Katholikentag ziehen und viele Anregungen und Fragen mitnehmen.

5 Ausblick

Im Jahr 2018 lag der Schwerunkt der Arbeit des Katholischen Datenschutzzentrums durch die Einführung der neuen Regelungen zum Datenschutz eindeutig auf der Beratung und Information zur neuen Gesetzeslage und den Auswirkungen für die kirchlichen Stellen.

Nachdem wir zum Ende des Jahres den Höhepunkt an Beratungsanfragen deutlich überschritten hatten und zur Mitte 2019 bzw. zum Jahresende 2019 Übergangsfristen zur Umsetzung des neuen Gesetzes ablaufen werden, wird der Fokus des Katholischen Datenschutzzentrums ab dem zweiten Halbjahr auch wieder stärker auf der Überprüfung der Einhaltung der Regelungen durch die kirchlichen Einrichtungen liegen. Das Katholische Datenschutzzentrum plant hierbei sowohl Querschnittsprüfungen zu allgemeinen Fragen bis hin zu Vor-Ort-Prüfungen in Einzelfällen.

Mit der ab dem 01. März 2019 geltenden neuen Durchführungsverordnung zum KDG wird aber auch der beratende Teil der Arbeit des Katholischen Datenschutzzentrums auf einem hohen Niveau bleiben.

Auch plant das Katholische Datenschutzzentrum den kirchlichen Einrichtungen weiterhin als Ansprechpartner auf vielen Veranstaltungen zur Verfügung zu stehen und über den kirchlichen Datenschutz zu informieren.

Mit unserer Veranstaltung „Ein Jahr Gesetz über den Kirchlichen Datenschutz (KDG) – Rückblick und Ausblick“ am 28. Mai 2019 in Siegburg wollen wir mit hochrangigen Referenten ein erstes Resümee nach einem Jahr KDG ziehen, aber auch nach vorne schauen auf das, was noch kommt.

6 Anhang Beschlüsse der Konferenz der Diözesandatenschutz-beauftragten im Jahr 2018

6.1 Weitergabe personenbezogener Daten an Kirchenzeitungsverlage zu Werbezwecken

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 08. Februar 2018)

Die Konferenz stellt die datenschutzrechtliche Unzulässigkeit der Weitergabe von personenbezogenen Daten/ Meldedaten eines (Erz-) Bistums zum Zweck der Werbung für eine Kirchenzeitung an die jeweiligen Verlage fest.

6.2 Mindestinhalte der Fachkunde betrieblicher Datenschutzbeauftragter

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 08. Februar 2018)

Da an die Diözesandatenschutzbeauftragten vermehrt die Frage herangetragen wurde, was die „zur Erfüllung seiner Aufgaben notwendige Fachkunde" des betrieblichen Datenschutzbeauftragten (bDSB) gem. §36 Abs. 6 KDG umfasst.

Die Konferenz der Diözesandatenschutzbeauftragten weist darauf hin, dass der Umfang der notwendigen Kenntnisse z.B. durch die Art der Aufgaben des Verantwortlichen und die Kritikalität der verarbeiteten Daten oder einrichtungsspezifische Besonderheiten der Datenverarbeitung beeinflusst wird und zusätzliche Kenntnisse erfordern kann.

Insbesondere über nachfolgende Punkte sollte sich der betriebliche Datenschutzbeauftragte informiert haben:

A. Grundlagen der Arbeit

1. Struktur kirchlicher Entscheidungen
2. Kirchliche Gesetzgebung / verfassungsrechtliche Grundlagen
3. Subsidiaritätsprinzip (§ 2 Abs. 2 KDG) / Zusammenspiel mit staatlichen Gesetzen

B. Rechtliche Aspekte
1. KDG inkl. DVO und der KDSGO
2. Nebengesetze (KMAO, KAO, andere diözesane Regelungen)
3. Einschlägige Regelungen der nicht-kirchlichen Gesetze (z.B. SGB, BMG, DSGVO, BDSG)
4. Unterschiede zwischen KDG und DSGVO bzw. dem BDSG
5. Spezialfall: Auftragsverarbeitung / Funktionsübertragung

C. Technische Aspekte
1. Grundlagen der IT
2. Aspekte der IT-Sicherheit
3. Technisch-organisatorische Schutzmaßnahmen
4. Grundlegendes Verständnis von BSI-Grundschutz / ISO 2700x / ISIS 12

D. Organisation der Arbeit
1. Rechte des bDSB
1.1. Kündigungsschutz
1.2. Direkter Berichtsweg zur Leitung der Einrichtung
1.3. Notwendigkeit der Einbindung in die Prozesse der Einrichtung / Beteiligung nach § 38 Satz 2 Buchst. a KDG)
1.4. Einsichtsrechte
2. Pflichten des bDSB
2.1. Verschwiegenheitspflicht nach § 43 Abs. 9 KDG
2.2. Meldepflicht nach § 36 Abs. 4 KDG
2.3. Fortbildung / Erhalt der Fachkunde nach § 37 Abs. 2 KDG
2.4. Überwachung ordnungsgemäße Anwendung DV-Programme (§ 38 Satz 2 Buchst. a KDG)
2.5. „Vertraut machen" der Mitarbeiter / Mitarbeiterinnen (Schulung) mit Regelungen (§ 38 Satz 2 Buchst. c KDG)
3. Vernetzungsmöglichkeiten und -pflichten des bDSB
3.1. … mit internen Stellen (z.B. MAV, Revision, Rechtsabteilung oder QM)
3.2. … mit der Aufsicht (§ 38 Satz 1 und Satz 2 Buchst. e KDG)
3.3. … mit anderen externen Stellen (z.B. Arbeitskreise, Erfahrungsaustauschkreise)
4. Wichtige „Werkzeuge"
4.1. Bestandsaufnahme / Schwachstellenanalyse
4.2. Verfahrensverzeichnis
4.3. Datenschutzfolgenabschätzung
4.4. Dokumentation der Datenverarbeitung (Accountability) für die Arbeit des bDSB nutzen
5. Beherrschung des Handwerkszeuges
5.1. Empfehlung zur risikoorientierten Herangehensweise an die Bewertung von Sachverhalten im Datenschutz / Erstellung + Umsetzung individueller Maßnahmenkatalog
5.2. Informationsquellen finden und nutzen

Für den Nachweis der Fachkunde ist keine Zertifizierung notwendig. Der Besuch entsprechender Seminare oder der Erwerb der Fachkunde auf andere Weise reicht aus. Dies muss aber nachvollziehbar bzw. nachweisbar sein. Besuchte Schulungen / Seminare zum BDSG (neu) bzw. zur DSGVO werden für die Fachkunde anerkannt, wenn das Wissen um die kirchlichen Spezifika im Allgemeinen und des KDG im speziellen anderweitig erworben wurde Der zeitliche Umfang der Vermittlung bzw. Aneignung dieser Grundlagen sollte in einem angemessenen Verhältnis zu den Inhalten stehen.

6.3 Muster Benennung betrieblicher Datenschutzbeauftragter

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 17. und 18. April 2018)

Die Konferenz der Diözesandatenschutzbeauftragten beschließt das Muster „Benennung betrieblicher Datenschutzbeauftragten in der beigefügten Fassung.

Muster zur Benennung von betrieblichen Datenschutzbeauftragten

Sehr geehrte(r) Herr/Frau _____,

mit Wirkung zum xx.xx.xxxx werden Sie gemäß § 36 KDG zum betrieblichen Datenschutzbeauftragten der Name der Einrichtung-Einrichtung in _____ benannt.

In dieser Funktion sind Sie weisungsfrei.

Ihre Aufgabe ist es, unbeschadet der eigenen Datenschutzverantwortung der Verantwortlichen, in Ihrer Einrichtung, durch Beratung und jederzeitige auch unangemeldete Kontrollen, auf die Einhaltung des KDG sowie anderer Rechtsvorschriften über den Datenschutz hinzuwirken.
m Einzelnen ergeben sich Ihre Aufgaben aus § 38 KDG.

Sie sind bei der Erfüllung Ihrer Aufgaben von allen Mitarbeitenden sowie von der Einrichtungsleitung zu unterstützen.

In dieser Funktion sind Sie der Leitung unmittelbar unterstellt.

Alle Mitarbeitenden der Einrichtung können sich in Angelegenheiten des Datenschutzes unmittelbar an Sie wenden. Die vertrauliche Behandlung der Einwendungen ist durch die Einrichtungsleitung sicher zu stellen.
Ihre Rechtstellung ergibt sich aus § 37 KDG.

Mit freundlichen Grüßen

6.4 Haftung des betrieblichen Datenschutzbeauftragten

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 17. und 18. April 2018)

An die Konferenz der Diözesandatenschutzbeauftragten sind immer wieder Fragen zur Haftung des betrieblichen Datenschutzbeauftragten gestellt worden. Die Konferenz hat sich mit der Problematik befasst und in der Sitzung vom 17. und 18. April 2018 folgenden Beschluss verfasst.

Haftung betrieblicher Datenschutzbeauftragter

Zum betrieblichen Datenschutzbeauftragten kann ein Mitarbeiter bestellt werden (interner betrieblicher Datenschutzbeauftragter) oder ein externer Anbieter (externer Datenschutzbeauftragter).

1. Strafrechtliche Haftung

Eine solche scheidet regelmäßig für den betrieblichen Datenschutzbeauftragten aus, da er in der Regel keine Garantenpflicht hat. Eine Ausnahme bildet die Strafbarkeit nach §203 StGB, wenn der bDSB ein fremdes Geheimnis offenbart, von dem er während seiner Tätigkeit erfahren hat. In dieser Hinsicht spielt die Frage der internen oder externen Bestellung keine Rolle.

2. Zivilrechtliche Haftung

2.1. Ansprüche des Betroffenen

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

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

2.2. Ansprüche der verantwortlichen Stelle

2.2.1. Ansprüche gegenüber dem internen BDSB

Hinsichtlich einer Haftung gemäß §280ff. BGB ist zu berücksichtigen, dass eine Haftungserleichterung im Arbeitsrecht nach §619 BGB besteht. Der Arbeitgeber müsste dem Arbeitnehmer sein Verschulden beweisen.

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

2.2.2. Ansprüche gegenüber dem externen bDSB
Die Haftung ergibt sich aus den Regelungen des Geschäftsbesorgungsvertrages. Eine dem § 619a BGB vergleichbare Regelung fehlt.

Auch Haftungserleichterungen sind in diesem Fall nicht vorgesehen.

2.3.
Für beide Fälle gilt jedoch, dass eine Haftung des bDSB nur dann in Betracht kommt, wenn diesem von der verantwortlichen Stelle alle erforderlichen Informationen über die Datenverarbeitung gewährt worden sind.

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

6.5 Verträge zur Auftragsverarbeitung mit externen Unternehmen

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 17. und 18. April 2018)

An die Konferenz der Diözesandatenschutzbeauftragen sind vermehrt Anfragen gestellt worden, wie die im §31 Abs. 2 KDG aufgestellte Anforderung zur vertraglichen Verpflichtung des Auftragsverarbeiters auf das KDG zu verstehen und umzusetzen sei.
Die Konferenz hat sich mit der Fragestellung in der Sitzung vom 17. und 18. April 2018 befasst und folgenden Beschluss verfasst.

Verträge zur Auftragsverarbeitung mit externen Unternehmen

Bei Abschluss von Verträgen kirchlicher Dienststellen mit externen Unternehmen soll eine Bezugnahme auf das aktuelle KDG in den Vertragstext aufgenommen werden, um § 31 KDG zu erfüllen.

6.6 Leitfaden elektronische Kommunikation

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 17. und 18. April 2018)

Mit diesem Leitfaden soll auf praxisrelevante Fragestellungen und Themen eingegangen werden, die sich beim täglichen Umgang mit elektronischer Kommunikation und der Verwendung externer Speichermöglichkeiten, also z.B. Speicherorten in der „Cloud" ergeben.

Das Ziel ist, das Bewusstsein für datenschutz- und datensicherheitsbezogene Risiken zu schärfen und jeweils passende Handlungsempfehlungen zu geben, durch deren Befolgen die Risiken deutlich begrenzt werden können.

Datenschutzrechtlich bedeutsam ist bei der Kommunikation und bei der Speicherung im Wesentlichen, ob personenbezogene Daten so gespeichert oder übermittelt werden, dass eine unbefugte Offenlegung gegenüber Dritten nicht mit der erforderlichen Sicherheit ausgeschlossen werden kann. Das ist meist aber keine Frage, die schnell mit einem bloßen Ja oder Nein beantwortet werden kann, sondern eine Gesamtabwägung aller Umstände verlangt. Erfahrungswerte sprechen vielfach dafür, dass kirchliche Dienststellen sich eher Risiko-avers verhalten sollten, d.h. Risiken für die Integrität und Vertraulichkeit der Daten eher vermeiden sollten als diese Risiken zugunsten einer größeren Bequemlichkeit zu akzeptieren.

Es müssen also – auch und gerade im Hinblick auf § 26 Abs. 3 KDG (bisher § 6 KDO) – vor der beabsichtigten Handlung die Prozessschritte des klassischen Risikomanagements durchgeführt werden:

- Risiko-Identifizierung: Welche Risiken für personenbezogene Daten bestehen. Welcher Schaden oder welche Gefährdung kann für den Betroffenen durch eine nicht autorisierte Offenlegung seiner Daten eintreten?

- Risiko-Bewertung: Wie groß wäre der potentielle Schaden und mit welcher Wahrscheinlichkeit wird sich das Risiko realisieren?

- Risiko-Abwehr: Welche Maßnahmen können ergriffen werden, um das Risiko hinsichtlich seiner Wahrscheinlichkeit und/oder seiner Schadenshöhe zu reduzieren oder sogar auszuschließen?

Die Tabelle in diesem Leitfaden soll helfen, die Risiken in ihrer Komplexität zu verstehen und Abhilfe zu schaffen. Dabei wurde auf eine detaillierte Bewertung der Risiko Wahrscheinlichkeiten verzichtet, weil diese sehr vom Einzelfall abhängt und aufgrund der Schwere der potentiellen Schäden oft auch geringste Eintrittswahrscheinlichkeiten das Risiko schon inakzeptabel machen.

Die empfohlenen Maßnahmen sind aus unserer Sicht verhältnismäßig im Hinblick auf Ihre Implementierungskosten und den zu tragenden organisatorischen Aufwand und entsprechen dem Stand der Technik. Demnach erfüllen sie die Vorgaben des § 26 Abs. 3 KDG.

Ein Verzichten auf diese Maßnahmen mit Berufung auf eine vorliegende Einwilligung des Betroffenen in einen „unsicheren" Umgang mit seinen personenbezogenen Daten halten wir nur in wenigen Ausnahmefällen für angebracht, da ein solches Vorgehen dem Selbstverständnis von kirchlichen Einrichtungen in diesen elementaren Fragen des Daten- und Vertrauensschutzes widerspricht.

Thema / Subjekt	Risikobeschreibung	Relevante Rechtliche Bestimmungen oder Grundsätze	Maßnahmen zur Erreichung der Konformität oder Risikominderung
Festnetz-telefonie	Herkömmliche analoge Telefonie sowie Router-gebundenes VOIP bei etabliertem Anbieter ist risikoarm, weil zeitgemäße Verschlüsselungstechniken verwendet werden	TKG, DSGVO	
Mobieltelefonie, mobile Daten-verbindung	Telefonate und UMTS- bzw. LTE- Datenverbindungen eher unproblematisch, aber Nutzung (z.B. von VOIP) in öffentlichen WLAN sehr risikobehaftet (unbefugtes Mithören/Mitlesen, z.T. selbst bei verschlüsselten Netzen durch Sicherheitslücke während des Verbindungsaufbaus.	§§ 26, 27 KDG	VPN-Tunnel bei der Nutzung öffentlicher Netze. Ansonsten öffentliche WLAN möglichst vermeiden.
SMS / MMS	Basiert auf mobiler Telefonie, deshalb relativ sicher		
Telefax	Historisch ein sicheres und zugelassenes Medium, solange die Übertragung auf der klassischen analogen Telefonie basierte. Wegen der immer weiter verbreiteten (und für den Anwender transparenten) Verbreitung der digitalen Übertragung (IP) ähnelt das Telefax in Datenschutz-Hinsicht inzwischen der E-Mail. Durch Integration in Kombi-Geräte (Gemeinschaftsdrucker) kann die Vertraulichkeit zusätzlich kompromittiert werden.	Vertraulichkeit	Faxgeräte nur als Einzelgeräte einrichten oder vertraulichen Druck als Voreinstellung vorgeben. Wenn analoge Übertragung nicht garantiert werden kann, besser vermeiden (und stattdessen verschlüsselte E-Mail nutzen)

Thema / Subjekt	Risikobeschreibung	Relevante Rechtliche Bestimmungen oder Grundsätze	Maßnahmen zur Erreichung der Konformität oder Risikominderung
Soziale Netzwerke und deren verbundene Messenger-Dienste	Unkontrollierbare Übertragung und Verwertung der Daten und Metadaten, auch in Drittstaaten, auch von Unbeteiligten durch Auslesen von Adressbüchern	§§ 39-41 KDG bzw. ein möglicher Verstoß gegen diese Drittlandsbestimmungen	Strikte Trennung zwischen privaten und dienstlichen Daten per Technik und Dienstanweisung. I.d.R. keine dienstliche Nutzung
Andere Messenger-Dienste	Eventuell fehlende Datenschutz-Konformität	KDG	Datenschutz-Faktoren wie Verschlüsselung, Vertraulichkeit, Speicherort sind streng zu prüfen. Dienstliche und private Nutzung sind streng zu trennen, d.h. separate Geräte, kein „Bring your own device“.
FTP (File transfer protocol)	Unverschlüsselte Datei-Übertragung, dadurch Möglichkeit des Mitlesens und der Verfälschung	§§ 26, 27 KDG Vertraulichkeit, Integrität	Entweder Dateien vor dem Übertragen verschlüsseln, oder nur per VPN-Tunnel übertragen oder SFTP (Secure file transfer protocol) verwenden, welches eine Transportverschlüsselung einschließt.

Thema / Subjekt	Risikobeschreibung	Relevante Rechtliche Bestimmungen oder Grundsätze	Maßnahmen zur Erreichung der Konformität oder Risikominderung
E-Mail	Möglichkeit des Mitlesens in jedem Vermittlungsknoten („Elektronische Postkarte“). Möglichkeit der Fälschung von Absenderangaben. Auch beste Absicherungen (siehe rechte Spalte) auf nur einer der beiden Seiten (Sender oder Empfänger) können durch Schwachstellen auf der jeweils anderen Seite unwirksam gemacht werden.	Vertraulichkeit, Integrität, Authentizität	E-Mail verschlüsseln und signieren. (Beispiel: S/MIME oder PGP) Ansonsten nur unkritische Inhalte per offener E-Mail übertragen. Bei Inhalten mit personenbezogenen Daten zuvor die Einwilligung des Betroffenen zur Übertragung einholen. Risiko-Reduzierung durch - Nutzung seriöser inländischer, bestenfalls kirchlicher Provider - Nutzung virtueller privater Netzwerke (VPN) für die Übermittlung vom/zum Provider **Die beiden vorstehend genannten Maßnahmen sind nur dann voll wirksam, wenn sie sowohl auf Sender- als auch auf Empfängerseite beachtet werden!** - Dateitransfer per gesichertem Download/Upload von der Website (wie z.B. bei Kontoauszügen) - Bereitstellen von Kontaktformularen auf der (verschlüsselten) Website

Thema / Subjekt	Risikobeschreibung	Relevante Rechtliche Bestimmungen oder Grundsätze	Maßnahmen zur Erreichung der Konformität oder Risikominderung
Fernwartung einer EDV-Anlage mit gespeicherten personenbezogenen Daten.	Während der Fernwartung kann es zu unbeabsichtigten und unkontrollierten Offenlegungen gegenüber dem Servicetechniker kommen. Der Tatbestand der Auftragsverarbeitung wird nicht erkannt. Notwendige vertragliche Regelungen unterbleiben.	§§ 10,29 KDG	§ 29 Abs. 12 KDG definiert die Fernwartung als besondere Art der Auftragsverarbeitung. Demnach ist ein Auftragsverarbeitungsvertrag mit dem Erbringer der Fernwartung abzuschließen, der alle Anforderungen des § 29 KDG erfüllt.
Nutzung einer Cloud mit physikalischer Datenspeicherung im Ausland, (z.B. MS One Drive, Dropbox, Google) oder mit nicht definiertem oder unklarem physikalischem Speicherort.	Bei physikalischer Speicherung der Daten in einem Drittland ist u.U. kein mit der Eu-DSGVO und dem KDG vergleichbares Datenschutzniveau gewährleistet. Möglicher Verstoß gegen Drittlandsbestimmungen.	§§ 39-41 KDG	Verwendung einer Cloud mit physikalischer Speicherung innerhalb der EU oder in Ländern mit durch die EU anerkanntem Datenschutzniveau (Angemessenheitsbeschluss). In Ausnahmefällen: Dokumentation der Abwägung der Ausnahmebedingungen nach § 41 KDG.

Thema / Subjekt	Risikobeschreibung	Relevante Rechtliche Bestimmungen oder Grundsätze	Maßnahmen zur Erreichung der Konformität oder Risikominderung
Auftragsverarbeitung von Daten, die in § 203 StGB genannt sind (Amts- und Berufsgeheinisse, v. a. medizinische Daten).	Erhöhtes Risiko der unzulässigen Offenlegung durch Verlängerung der Verarbeitungskette. Nicht ausreichende oder fehlerhafte Vertragsgestaltung kann auch strafrechtlich relevant werden	§ 203 StGB, § 29 KDG	Prinzipiell ist die Auftragsverarbeitung personenbezogener Daten im Zusammenhang mit Amts- und Berufsgeheimnissen zulässig, wenn verschärfte Anforderungen an ▪ die Gestaltung des Auftragsverarbeitungsvertrages ▪ die Einbindung der Mitarbeiter des Auftragsverarbeiters (Verschwiegenheitserklärung) ▪ die Einhaltung der Drittlandsbestimmungen beachtet werden.

6.7 Veröffentlichung von Fotos von Kindern und Jugendlichen unter 16 Jahren

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 17. und 18. April 2018)

Die Konferenz der Diözesandatenschutzbeauftragten beschließt, dass zumindest für die Veröffentlichung von Bildern von Kindern bis zur Vollendung des 16. Lebensjahres die vorherige Einwilligung der Sorgeberechtigten unter Vorlage der jeweils zur Veröffentlichung vorgesehenen Bilder einzuholen ist. Der Beschluss korrespondiert mit der Entschließung der Konferenz der Beauftragten für den Datenschutz der EKD vom 12.04.2018, dem sich die Konferenz anschließt.

Erläuterungen zu Fragen des Umgangs mit Bildern und Fotografien

Mit dem Inkrafttreten des neuen Gesetzes über den Kirchlichen Datenschutz (KDG) sind die Anforderungen an die Zulässigkeit des Fotografierens bei kirchlichen Veranstaltungen und Ereignissen erheblich angestiegen. Entgegen aller Befürchtungen ist es aber auch nach dem KDG nach wie vor möglich, bei diesen Anlässen zu fotografieren, ohne dass von jedem Einzelnen eine entsprechende Einwilligungserklärung nachzuweisen ist. Das Fotografieren im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten unterliegt dabei nicht den Vorgaben des KDG. Etwas anders gilt aber, wenn die Verarbeitung im Rahmen der Tätigkeit eines Verantwortlichen einer Dienststelle erfolgt.

Rechtsgrundlagen

In der Regel werden beim Fotografieren von Menschen dann personenbezogene Daten erhoben, wenn die Bilder digital (§ 2 Abs. 1 KDG) im Sinn einer automatisierten Verarbeitung aufgenommen werden und zur Identifikation des Aufgenommenen geeignet sind. Die Verarbeitung personenbezogener Daten ist aber nur unter bestimmten Voraussetzungen datenschutzrechtlich zulässig. In Übereinstimmung mit der EU – DSGVO gilt auch im KDG weiterhin das Verbot mit Erlaubnisvorbehalt, welches besagt, dass eine Verarbeitung personenbezogener Daten generell nur durch eine Rechtfertigung möglich ist. Das heißt, Bildaufnahmen sind zunächst nach § 6 Abs. 1 KDG verboten, wenn sie nicht auf eine Rechtfertigung gestützt werden können - dies kann entweder eine gesetzliche Grundlage oder eine Einwilligung des Betroffenen in die Verarbeitung sein.

1. Erheben und Speichern

Als gesetzliche Grundlage, nach der das Erheben und Speichern von Bildern zulässig sein kann, kommen mehrere Regelungen in Frage:

▪ die Aufgabenzuweisungsnorm, wegen der eine Handlung im kirchlichen Kontext vorgenommen wird: Dabei ist aber auf genaue Ermächtigung für die Verarbeitung personenbezogener Daten zu achten. Z.B. ist die Aufnahme der Daten des Kindes und der Eltern bei der Anmeldung des Kindes zur Taufe von den entsprechenden Regelungen gedeckt. Ob hierzu auch die Anfertigung eines Fotos durch die Pfarrgemeinde von der Taufe gehört, ist im Einzelfall zu prüfen.

▪ § 6 Abs. 1 lit. f) KDG: Die Regelung ermöglicht dann eine Verarbeitung, wenn sie zur Wahrnehmung einer Aufgabe dieser Stelle erforderlich ist und die Aufgabe im kirchlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dieser Stelle (dem Verantwortlichen) übertragen wurde. Auch hier bedarf es wieder eines Handelns innerhalb einer zugewiesenen Aufgabe. Außerdem muss die Verarbeitung für die Aufgabenwahrnehmung erforderlich sein. Dies bedeutet, dass eine Abwägung zwischen dem Mittel der Datenverarbeitung und dem damit verfolgten Zweck zu erfolgen hat.

▪ § 6 Abs. 1 lit. g) KDG: Inhaltlich wird darin gefordert, dass die Verarbeitung bei Vorliegen eines berechtigten Interesses immer eine Abwägung mit dem Interesse oder den Grundrechten bzw. Grundfreiheiten der betroffenen Person erforderlich macht. Zu den „berechtigten Interessen" zählen nicht nur rechtliche, sondern auch tatsächliche, wirtschaftliche oder ideelle Interessen. Bloße Allgemeininteressen reichen demgegenüber nicht aus (vgl. Kühling-Buchner, Kommentar zur Datenschutzgrundverordnung, Art. 6 DSGVO Rdnr. 146).
Gegen das berechtigte Interesse des Fotografen ist das schutzwürdige Interesse der betroffenen Person im konkreten Einzelfall abzuwägen. Je intensiver der Eingriff in die Interessen oder Grundrechte der betroffenen Person sind, desto stärker sind dann die Rechte und Interessen der betroffenen Person zu berücksichtigen. Soweit die Abwägung dazu führt, dass die Aufnahme durch das berechtigte Interesse des Fotografen gedeckt ist, bedarf es insoweit keiner gesonderten Einwilligung des Betroffenen mehr. Es ist davon auszugehen, dass die notwendige Abwägung im gleichen Sinn auch dazu führen wird, die Aufnahme auf dem digitalen Fotoapparat zu speichern. Bitte beachten Sie: Soweit eine öffentlich-rechtlich organisierte kirchliche Stelle im Rahmen ihrer Aufgaben handelt, kann sie diese Ermächtigung nicht nutzen (siehe § 6 Abs. 1 lit. g) Satz 2 KDG).

2. Veröffentlichung von Bildern

Neben dem Erheben und Speichern ist auch die Rechtmäßigkeit der Veröffentlichung als gesonderter Verarbeitungsvorgang zu prüfen.

Dabei können die schon für das Erheben und Speichern der Fotos in Frage kommenden Ermächtigungsgrundlagen wieder herangezogen werden.

Die Veröffentlichung von Bildern zum Beispiel im Internet kann – soweit es nicht zur Aufgabe einer öffentlich-rechtlich organisierten kirchlichen Stelle gehört (s.o.) - ebenfalls nach § 6 Abs. 1 lit. g) KDG rechtmäßig sein. Es ist wiederum eine Abwägung erforderlich, bei der im Hinblick auf die Intensität des Eingriffes in die Interessen oder Grundrechte des Betroffenen auch die Form der beabsichtigten Veröffentlichung mit zu berücksichtigen ist. Als Hilfestellung bei der Interessenabwägung können unabhängig davon, ob das Kunsturhebergesetz (KUG) neben dem KDG Anwendung findet, zumindest die dort genannten Kriterien und die dazu ergangenen Entscheidungen der Gerichte dienen. Beispielsweise wenn Bildnisse aus dem Bereich der Zeitgeschichte veröffentlicht werden oder Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstige Örtlichkeiten erscheinen, spricht das wohl dafür, dass die Abwägung mit den Betroffenenrechten zugunsten der Interessen des Fotografen an einer Veröffentlichung ausgehen kann. Gleiches gilt für Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben oder für Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient. Auf der anderen Seite spricht beispielsweise vieles dafür, dass nicht mehr von einem bloßen Beiwerk im Rahmen der Aufnahme auszugehen ist, wenn einzelne Personen hervorgehoben werden oder einzelne oder wenige Personen Gegenstand der Bilder sind.

3. Schutz Minderjähriger

Parallel zur EU - DSGVO hat der kirchliche Gesetzgeber in § 6 Abs. 1 lit. g) KDG geregelt, dass im Rahmen der erforderlichen Abwägung von einer überwiegenden Schutzbedürftigkeit der Betroffeneninteressen insbesondere dann auszugehen ist, wenn es sich bei der betroffenen Person um einen Minderjährigen handelt. Die generelle Schutzbedürftigkeit von Minderjährigen (unter 18 Jahre) schließt es auch nicht aus, im Rahmen der konkreten Interessensabwägung auf das jeweilige Alter der betroffenen Kinder abzustellen und hier je nach Alter die Schutzbedürftigkeit entsprechend höher oder niedriger einzustufen. Mit Blick auf die Wertung des Art. 8 Abs. 1 EU-DSGVO (entsprechend § 8 Abs. 8 KDG) ist dabei noch einmal die Vollendung des sechzehnten Lebensjahres als Abwägungskriterium von zentraler Bedeutung.

Bei Kindern unter sechzehn Jahren geht die EU - DSGVO von einer besonderen Schutzbedürftigkeit aus, die es erforderlich macht, bei der Ausübung informationeller Selbstbestimmung auf Grundlage des Art. 8 Abs. 1 EU – DSGVO grundsätzlich die Personenfürsorgeberechtigten mit einzubinden. Dementsprechend ist dann auch im Rahmen der Interessensabwägung davon auszugehen, dass hier regelmäßig die schutzbedürftigen Interessen des betroffenen Kindes überwie-

gen (vgl. Kühling-Buchner Art. 6 DSGVO Rdnr. 155). So ist es auch bei der Abwägung nach § 6 Abs. 1 lit. g) KDG. Die katholischen Datenschutzaufsichtsbehörden haben dem Rechnung getragen und im Rahmen einer generellen Abwägung das berechtigte Interesse der Verantwortlichen an der Veröffentlichung von Bildern zugunsten der schutzbedürftigen Interessen der Kinder und Jugendlichen bis zum vollendeten sechzehnten Lebensjahr zurückgestellt. In Ermangelung einer anderen Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten (= Erheben, Speichern, Veröffentlichen usw.) kann eine solche nur im Rahmen einer Einwilligung erfolgen, die den Anforderungen des KDG genügen muss. (einstimmiger Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 17.04.2018).

4. Informations- und Transparenzpflichten

Wenn bei Aufzügen, bei Veranstaltungen oder ähnlichen Ereignissen eine unüberschaubar große Menge von Menschen fotografiert wird, ist es naheliegend, dass die Verarbeitung der Daten derjenigen, die als Beiwerk abgelichtet werden, nicht mit deren Kenntnis erfolgt. Das bedeutet, die Informationspflichten, die bei unmittelbarer Datenerhebung nach § 15 KDG ausgelöst würden, treten hier nicht ein. Demgegenüber treten die Transparenzpflichten nach § 16 KDG bei mittelbarer Datenerhebung ein. Die insoweit vorhandenen Informationspflichten können aber nach § 16 Abs. 4 lit. b) KDG zurücktreten, wenn sich die Erteilung der Information aufgrund der unüberschaubaren Menge der Betroffenen als unmöglich erweist oder einen unverhältnismäßig großen Aufwand erforderlich machen würde. Bei der Beurteilung sind jeweils die Umstände des Einzelfalls maßgeblich. Es gilt also keineswegs generell, dass die Informationspflichten zurücktreten. Abhängig vom tatsächlichen Bild kann es auch beim Fotografieren von Sehenswürdigkeiten oder Veranstaltungen mit einem vertretbaren Aufwand möglich sein, die Informationspflichten nach § 16 KDG bei der Erhebung der personenbezogenen Daten zu erfüllen. Dies hat zur Folge, dass die vorgenannte Ausnahme nicht eintreten kann.

Die Informationserteilung muss auch nicht zwangsläufig durch den Fotografen erfolgen. Bei Veranstaltungen ist es beispielsweise möglich, dass der verantwortliche Veranstalter die Teilnehmer über die Anfertigung von Fotografien informiert. Ist eine solche Information aufgrund der Struktur der Veranstaltung von vorneherein unmöglich, spricht vieles dafür, dass die Erfüllung der Informationspflicht einen unverhältnismäßig großen Aufwand erfordern würde. Wenn die Umstände des Einzelfalls so sind, dass aus den genannten Gründen eine Informationspflicht zurücktreten kann, ist es dem Fotografen nicht zumutbar, im Nachhinein die von seinen Aufnahmen erfassten Personen zu identifizieren, um ihnen die nach dem kirchlichen Datenschutzgesetz grundsätzlich zustehenden Informationen zukommen zu lassen. Nach § 13 KDG ist er nicht verpflichtet, zur Einhaltung dieses Gesetzes zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffenen Personen zu informieren. Wird demge-

genüber eine überschaubare Menge von Personen fotografiert, ist der Fotograf natürlich verpflichtet, seinen Informationspflichten nach § 16 KDG nachzukommen.

Diese Bewertung des Umgangs insbesondere mit der Veröffentlichung von Fotos versteht sich als eine Erläuterung, welche ergänzt werden kann.

6.8 Beurteilung von Messenger- und anderen Social-Media-Diensten

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 26. Juli 2018)

Die Konferenz der Diözesandatenschutzbeauftragten beschließt die nachfolgende Kriterienliste.

Vorbemerkung

Die katholischen Datenschutzaufsichten haben nachfolgend die aus ihrer Sicht relevanten Kriterien für die Bewertung und die Auswahl eines geeigneten Messenger-Produktes unter Datenschutz-Gesichtspunkten zusammengestellt. Neben diesen können aber auch andere Kriterien eine Rolle spielen, deren Erfüllung für die legale Verbreitung im kirchlichen Raum förderlich ist.

Kriterien, die ein Dienst aus Sicht des Datenschutzes erfüllen muss

▪ **Serverstandort**: Wo verarbeitet der Dienst-Anbieter die Nutzerdaten? Hält der Provider die Drittlandbestimmungen ein, d.h. keine Datenspeicherung außerhalb der EU bzw. nur in Ländern, deren Datenschutzniveau durch die EU anerkannt ist?

Aus §§ 39-41 KDG ergibt sich, dass eine Verarbeitung personenbezogener Daten nur dann in einem Drittland, also außerhalb der EU, stattfinden darf, wenn besondere Bedingungen erfüllt sind. Das können ein Angemessenheitsbeschluss der Europäischen Kommission, geeignete Garantien (§ 40 KDG) oder eine explizite Einwilligung der betroffenen Person (§ 41 Abs. 1 KDG) sein. In jedem Fall führt die Verarbeitung in einem Drittland zu einem deutlich größeren Aufwand bei der Herstellung und Überprüfung der Rechtmäßigkeit der Verarbeitung. Schon aus diesem Grund sowie dem permanenten Risiko, dass die Rechtmäßigkeit durch Änderung z.B. der Gesetzeslage im Drittland entfällt, raten wir von der Verarbeitung in einem Drittland ab, wenn nicht gleichzeitig eine Verschlüsselung nach dem Stand der Technik angeboten wird. Der Standort in einem Drittland wird weniger problematisch, wenn der zentrale Server nur verschlüsselte Daten zur Weiterleitung erhält, weil der Anbieter dann schon aus technischen Gründen den Inhalt der Kommunikation nicht offenlegen kann.

▪ **Sicherer Datentransport**: Werden die Inhalte der Kommunikation Ende-zu-Ende verschlüsselt, also z.B. auch bei der Zwischenpufferung auf dem Server des Providers?

Nach § 26 KDG hat der Verarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau zu gewährleisten. Als geeignete Maßnahme wird unter anderem die Verschlüsselung personenbezogener Daten ausdrücklich genannt. § 27 KDG fordert, die Sicherheitsoptionen so zu gestalten, dass bereits durch die Voreinstellung das angemessene Schutzniveau gewahrt wird. Verschlüsselung darf deshalb nicht „optional zuschaltbar" sein, sondern sollte per Default vorgegeben werden. Die Sicherheit der Daten sollte auch nicht nur auf dem Transport, also auf dem Weg vom Endgerät des Senders über den zentralen Server bis zum Endgerät des Empfängers gewährleistet werden, sondern auch, wenn die Daten auf dem Endgerät angekommen sind, durch eine sichere Datenhaltung in der Applikation, die die Daten z.B. gegen ungewolltes Ausspähen durch andere Applikationen auf dem gleichen Endgerät schützt. Dem aktuellen Stand der Technik (im Jahr 2018) entsprechen Transport- und Inhaltsverschlüsselungen nach den Standards TLS 1.2 oder AES 256 bzw. 512-Bit ECC.

Falls vorhanden, sollten Zertifizierungen des Produktes oder des Anbieters durch unabhängige Institutionen in die Bewertung einfließen.

▪ **Datenminimierung**: Werden die Metadaten der Verbindung so bald wie möglich gelöscht?

Eine Beschränkung auf das für den Zweck der Verarbeitung notwendige Maß an personenbezogenen Daten wird in § 7, Abs.1 lit c) KDG gefordert. Die Beschränkung gilt für die Menge und den Zeitraum der Verarbeitung und Speicherung. Deshalb ist zu fordern, dass alle personenbezogenen Daten, also Inhalte und Verbindungsdaten der Kommunikation, sobald wie möglich gelöscht werden.

Eine extreme Datenminimierung zusammen mit einer starken Ende-zu-Ende Verschlüsselung führt dazu, dass der Provider selbst unter Zwang (z.B. durch staatliche Behörden) technisch nicht in der Lage ist, Daten herauszugeben. Ebenso laufen illegale Angriffe auf die zentralen Server in Leere.

▪ **Respektierung der Rechte Dritter**: Werden nur die Kontaktdaten der an der Kommunikation Beteiligten verwendet und behält der Anwender die Kontrolle über sein Telefonbuch, oder wird z.B. das komplette Telefonbuch an den Provider übermittelt und die Verantwortung für die Information der Betroffenen auf den Anwender abgewälzt?

Personenbezogene Daten müssen rechtmäßig und für den Betroffenen in nachvollziehbarer Weise verarbeitet werden. (§ 7 Abs. 1 KDG).

Der Betroffene hat nach §§ 14 und 15 KDG umfassende Rechte auf Information über den Umfang und die Art der Verarbeitung seiner Daten. Dagegen verstößt regelmäßig die Ausspähung von Adressen und Kontaktdaten des Telefonbuches durch allzu neugierige Applikationen. Manche Anbieter versuchen über die AGB, die Verantwortung für die Einholung einer Einwilligung der Dritten in die Weitergabe ihrer Daten dem Nutzer aufzubürden, was dieser in der Praxis aber nie leisten kann.

Weitere Kriterien

Zu dem erweiterten Kriterienkreis gehören zum einen die Kosten: Der Entscheider sollte prüfen, ob die Nutzung des Produktes idealerweise für den privaten Nutzer kostenfrei und für die nicht-private Nutzung, also z.B. durch eine kirchliche Einrichtung, relativ erschwinglich ist.

Darüber hinaus sind die Bedingungen der Lizenzvergabe zu prüfen, die meistens in den AGB geregelt wird. Manche Anbieter untersagen die nicht-private Nutzung, andere untersagen lediglich die kommerzielle Anwendung. Während das Produkt im ersten Fall auch durch ehrenamtliche Non-Profit-Organisationen nicht genutzt werden darf, können diese im zweiten Fall – abhängig von den Formulierungen der AGB - doch von einer bestimmungsgemäßen Nutzung ausgehen. Nicht-privaten Nutzern wird manchmal eine spezielle „Business-Lösung" angeboten, die aber oft mit höheren Lizenzkosten verbunden ist als die Privat-Anwendung. Einige Anbieter fordern ein Mindestalter der Nutzer von 16 oder sogar 18 Jahren, nochmals andere Anbieter stellen ihr Produkt nur für Nutzer mit Wohnsitz in bestimmten Staaten zur Verfügung.

Jeder Entscheider muss sich also ausführlich und umfassend über die Lizenzbedingungen der Produkte informieren.

6.9 Verwendung von Cookies in Homepages

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 26. Juli 2018)

Die Konferenz der Diözesandatenschutzbeauftragten empfiehlt bei der Gestaltung der Datenschutzerklärung auf der Homepage die Einhaltung der nachfolgenden „Hinweise zur Verwendung von Cookies".

Hinweise zur Verwendung von Cookies

Datenschutzerklärungen stellen einen wesentlichen Bestandteil des Internetauftritts einer Einrichtung dar. Die bisherigen Regelungen des Telemediengesetzes werden ab dem 24. Mai 2018 durch die Vorschriften nach dem Gesetz über den Kirchlichen Datenschutz (KDG) ergänzt.

A. Informationspflichten

Nach § 15 KDG sind den Nutzern folgende Informationen zur Verfügung zu stellen:

- Namen, Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- Kontaktdaten des betrieblichen Datenschutzbeauftragten;
- der Zweck der Verarbeitung;
- die Rechtsgrundlage für die Verarbeitung;
- wenn die Verarbeitung auf § 6 Absatz 1 lit. g) KDG beruht, die berechtigten Interessen die verfolgt werden;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- die Speicherdauer der personenbezogenen Daten;
- Mitteilung über Betroffenenrechte;
- wenn die Verarbeitung auf Grund einer Einwilligung erfolgt, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird und
- das Bestehen eines Beschwerderechts bei der zuständigen Datenschutzaufsicht.

Je nach Gestaltung der Homepage sind folgende Informationen der Datenschutzerklärung hinzuzufügen:

- die Absicht des Verantwortlichen, die personenbezogenen Daten an oder in ein Drittland oder an eine internationale Organisation zu übermitteln sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission oder im Falle von Übermittlungen gemäß § 40 KDG einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist oder wo sie verfügbar sind.

- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß § 24 Absätze 1 und 4 KDG und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Die Darstellung der einzelnen Punkte in der Datenschutzerklärung sollte in sich logisch sein und den Nutzer darüber informieren, welche Cookies oder PlugIns jeweils genutzt werden.

B. Rechtmäßigkeit der Verarbeitung

Für die Rechtmäßigkeit der Verarbeitung kommen insbesondere § 6 Abs. 1 lit. g) KDG (Interessenabwägung), § 6 Abs. 1 lit. a) KDG (Einwilligung) und u.U. § 6 Abs. 1 lit. c) KDG (Vertragserfüllung) in Betracht.

1. Interessenabwägung

Die Interessenabwägung nach § 6 Abs. 1 lit. g) KDG als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommt insbesondere für die Webhoster sowie für technisch zwingend erforderliche Cookies in Betracht.

Webhosting meint lediglich, dass sich der jeweilige Betreiber einer Webseite der Unterstützung eines Dritten bedient, um dessen Speicherplatz zur Verfügung zu stellen. Im Rahmen dieses Webhostings werden regelmäßig personenbezogene Daten verarbeitet. Insbesondere stellt die ungekürzte IP-Adresse des Nutzers ein personenbezogenes Datum dar.

Ob eine Speicherung der ungekürzten IP-Adresse tatsächlich erforderlich ist, sollten Sie mit dem Webhoster besprechen. Dieser kann Ihnen hierzu auch weitere Informationen, insbesondere zum Zweck der Erhebung und Speicherung, zur Verfügung stellen.

Aufgrund des gesetzlich vorgesehen Grundsatzes der Datensparsamkeit nach § 7 Abs. 1 lit. c) KDG scheint es angemessen, die IP-Adresse derart zu kürzen, dass diese keiner natürlichen Person mehr zugeordnet werden kann (Anonymisierung). Die Anonymisierung stellt auch eine geeignete technische und organisatorische Maßnahme § 26 Abs. 1 S. 2 lit. a) KDG dar.

Technisch zwingend erforderliche Cookies sind beispielsweise die sogenannten SessionCookies. Diese sind in der Regel technisch notwendig, um die Funktion einer Webseite sicherzustellen und welche beim Ende des Nutzungsvorgangs automatisch gelöscht werden, somit nicht auf dem Computer der betroffenen Person verbleiben. Session Cookies dienen etwa der Speicherung von Log-in-Dateien, des Warenkorbs oder der Sprachauswahl.

Die Zuordnung , ob ein Cookie tatsächlich zwingend erforderlich ist, sollte sehr restriktiv erfolgen. Jedes „zu viel" kann im Rahmen der Interessenabwägung nach § 6 Abs. 1 lit. g) KDG auch zuungunsten der Einrichtung ausgelegt werden, sodass insoweit eine unrechtmäßige Verarbeitung personenbezogener Daten vorliegt.

2. Einwilligung
Eine Einwilligung ist immer dann erforderlich, wenn die Datenerhebung über das nach Punkt 1 erforderliche Maß hinausgeht. Bei den technisch nicht notwendigen Cookies handelt es sich mindestens um

- Tracking-Cookies,
- Targeting-Cookies,
- Analyse-Cookies und
- Cookies von Social-Media-Websites.

Hierzu zählen auch Codes, welche auf der jeweiligen Webseite eingebunden werden, um Neuigkeiten von Facebook und/oder Twitter unmittelbar auf der Homepage anzuzeigen.

Ein einfacher Hinweis in der Datenschutzerklärung reicht nicht mehr aus. Bereits beim ersten Aufruf der Homepage werden Daten erhoben und u.U. in die USA übermittelt oder durch Tracking-Tools der genaue Standort des Nutzers ermittelt.

Aus diesem Grund muss eine Einwilligung in die Datenverarbeitung nach § 8 KDG vorliegen, bevor eine Datenerhebung durch die vorgenannten und andere gleichartigen Cookies oder Codes erfolgt. Eine Einwilligung ist im Gegensatz zu einer Genehmigung auch immer vor der Datenerhebung zu erklären.

Eine Einwilligung kann durch unterschiedliche technische Maßnahmen in die Webseite eingebunden werden.

Eine Möglichkeit ist das „Zwei-Klick-Verfahren". Die Buttons, welche auf der Internetseite eingebunden werden, sind solange inaktiv, bis der jeweilige Nutzer diese manuell aktiviert. Das heißt, dass keine Datenübermittlung an Social-Media-Websites erfolgt, bis eine Einwilligung vorliegt.

Eine weitere Möglichkeit ist es, ein Cookie-Banner auf der Internetseite einzurichten. Dieser kann technisch so ausgestattet werden, dass keine Erhebung personenbezogener Daten erfolgt, bis auch hier eine Einwilligung des Nutzers vorliegt.

Die technischen Möglichkeiten sind vielseitig und können und sollen nicht abschließend dargestellt werden.

3. Vertragserfüllung
Ebenso kann für bestimmte Daten die Rechtmäßigkeit der Verarbeitung nach § 6 Abs. 1 lit. c) KDG gegeben sein.

Diese Rechtsgrundlage kommt etwa dann in Betracht, wenn Bestellprozesse über die Homepage abgewickelt werden sollen. So sind bestimmte Daten für den Vertragsschluss erforderlich, deren Erhebung nach § 6 Abs. 1 lit. c) KDG erforderlich ist.

6.10 Liste von Verarbeitungsvorgängen nach § 35 Abs. 5 KDG im Zusammenhang mit einer Datenschutz-Folgenabschätzung

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 26. Juli 2018)

Die Konferenz der Diözesandatenschutzbeauftragten beschließt und veröffentlicht die nachfolgende Liste von Verarbeitungsvorgängen nach § 35 Abs. 5 KDG.

Liste von Verarbeitungsvorgängen nach § 35 Abs. 5 KDG

A Gesetzliche Grundlage

Das Gesetz über den kirchlichen Datenschutz (KDG) regelt im § 35 „Datenschutz-Folgenabschätzung und vorherige Konsultation" die Rahmenbedingungen zur sog. Datenschutz-Folgenabschätzung (kurz: DSFA). Der § 35 KDG nennt dabei die Grundsätze, bei welchen Fällen eine DSFA durchzuführen ist und was diese enthält. Er beschreibtferner das besondere Verfahren der Konsultation des Verantwortlichen bei der Aufsichtsbehörde bei Fortbestehen hoher Risiken auch nach Anwendung der auf Grundlage der DSFA festgelegten verhältnismäßigen technischen und organisatorischen Maßnahmen.

Mit diesem Dokument kommen die Diözesandatenschutzbeauftragten dem Auftrag aus § 35 Abs. 5 KDG nach und legen eine Positivliste von Verarbeitungsvorgängen vor, bei denen aus Sicht der Diözesandatenschutzbeauftragten immer eine DSFA durchzuführen ist. Diese Liste orientiert sich an den bislang bekannten Vorgaben der staatlichen Aufsichtsbehörden.

Führt ein Verantwortlicher Verarbeitungsvorgänge aus, die in § 35 Abs. 4 KDG oder der vorliegenden Liste aufgeführt sind, ohne vorab eine DSFA durchgeführt zu haben, so kann die zuständige Datenschutzaufsicht wegen Verstoßes gegen § 35 Abs. 1 KDG von ihren Abhilfebefugnissen gemäß § 47 KDG einschließlich der Verhängung von Geldbußen gemäß § 51 KDG Gebrauch machen. Gegen einen derartigen Beschluss der Datenschutzaufsicht steht der Rechtsweg gemäß § 49 KDG offen.

Die in dem Dokument dargestellte Liste wird nachfolgend als „Muss-Liste" oder „Positiv-Liste" bezeichnet.

B Ziel dieses Dokuments

Ziel des Dokuments ist es, eine an den Listen der staatlichen Aufsichtsbehörden orientierte Liste zu entwickeln, die an die Situation der kirchlichen Einrichtungen im Geltungsbereich des KDG angepasst ist.

Auf Grund der Schnelllebigkeit im digitalen Umfeld kann dieses Dokument nur als „lebendiges" Papier angesehen werden, das ständigen Änderungskontrollen hinsichtlich der Aufnahme neuer Verarbeitungen

in die Liste der Verarbeitungsvorgänge unterliegt. Änderungen an Einträgen der Muss-Liste werden dokumentiert, so dass die Muss-Liste eine entsprechende Versionshistorie erhalten wird.

Wichtiger Hinweis: Wird die Verarbeitungstätigkeit eines Verantwortlichen in der vorliegenden Liste nicht aufgeführt, so ist hieraus nicht der Schluss zu ziehen, dass keine DSFA durchzuführen wäre. Stattdessen ist es Aufgabe des Verantwortlichen, als ersten Schritt einer DSFA einzuschätzen, ob die Verarbeitung aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen aufweist und damit die Voraussetzungen des § 35 Abs. 1 Satz 1 KDG erfüllt.

C Liste nach Art. 35 Abs. 5 KDG

Die „Artikel 29-Gruppe", der Vorläufer des Europäischen Datenschutzausschusses als Zusammenschluss aller nationalen Datenschutz-Aufsichtsbehörden in der EU, hat in seinem Working Paper (WP) 248 vom 4. April 2017 maßgebliche Kriterien zur Einordnung von Verarbeitungsvorgängen wie folgt formuliert:

1. Bewerten oder Einstufen (Scoring)
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische Überwachung
4. Vertrauliche oder höchst persönliche Daten
5. Datenverarbeitung in großem Umfang
6. Abgleichen oder Zusammenführen von Datensätzen
7. Daten zu schutzbedürftigen Betroffenen
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert

Erfüllt ein Verarbeitungsvorgang zwei oder mehr dieser Kriterien, so ist vielfach ein hohes Risiko gegeben und aus Sicht der Artikel 29-Gruppe eine DSFA durch den Verantwortlichen durchzuführen. In wenigen Einzelfällen mag es jedoch auch vorkommen, dass nur eines der genannten Kriterien erfüllt wird und dennoch auf Grund eines hohen Risikos des Verarbeitungsvorgangs eine DSFA notwendig wird.

Das Ergebnis dieses ersten Schrittes und die zugrundeliegenden Einschätzungen der im Zuge der Verarbeitungstätigkeit möglicherweise auftretenden Schäden sowie die resultierende Schwere und Eintrittswahrscheinlichkeit der Risiken sind zu dokumentieren.

Die folgende Liste von Verarbeitungsvorgängen einschließlich der genannten Beispiele ist nicht als abschließende Liste von Anwendungsfällen zu sehen, in denen einige der o.a. Kriterien als erfüllt erkannt werden, sondern soll beispielhaft verdeutlichen, in welchen Formen die Ausprägungen der Kriterien angetroffen werden können.

Dementsprechend ergibt sich für Verantwortliche, die prüfen, ob für einen Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung durchzuführen ist, die folgende Prüfreihenfolge:

1. Prüfung, ob der Verarbeitungsvorgang einen Fall nach § 35 Abs. 4 KDG darstellt oder in der folgenden Liste genannt ist.
2. Wenn nein, dann Prüfung anhand der o.a. Kriterien, ob dennoch ein hohes Risiko nach § 35 Abs. 1 KDG vorliegt.

Nur wenn beide Prüfungen negativ ausfallen, muss eine Datenschutz-Folgenabschätzung nicht durchgeführt werden.

Nach § 6 Abs. 1 KDG ist eine Verarbeitung nur dann rechtmäßig, wenn einer der dort genannten Erlaubnistatbestände vorliegt. Mit der vorliegenden Liste wird keine Aussage darüber getroffen, ob für einen Verarbeitungsvorgang eine Rechtsgrundlage vorliegt oder nicht. Ein Eintrag auf der Liste bedeutet daher weder, dass eine Verarbeitung verboten ist, noch dass ein Verarbeitungsvorgang allein auf der Grundlage einer Datenschutz-Folgenabschätzung durchgeführt werden kann.

Zum Aufbau der Liste: In der ersten Spalte erfolgt zur einfachen Bezugnahme eine Nummerierung. In der zweiten Spalte findet sich die maßgebliche Beschreibung des Verarbeitungsvorgangs. Fällt ein Verarbeitungsvorgang unter diese Beschreibung, dann ist für ihn eine Datenschutz-Folgenabschätzung durchzuführen. Lässt sich ein Verarbeitungsvorgang nicht unter die zweite Spalte subsumieren, ist nach dem oben dargestellten Schema weiter zu prüfen. Die dritte und die vierte Spalte enthalten zur Veranschaulichung typische Einsatzfelder und Beispiele für Verarbeitungsvorgänge – vorzugsweise aus dem kirchlichen Bereich - die unter die zweite Spalte zu subsumieren wären. In der fünften Spalte wird auf diejenigen der o.a. neun Kriterien referenziert, die bei dem jeweiligen Verarbeitungsvorgang typischerweise erfüllt werden und die deshalb dazu führen, den Vorgang in die Liste aufzunehmen.

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
1.	Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß §§ 11 und 12 KDG handelt.	Krankenhäuser, Praxisverbünde, Apothekendienste Sozialleistungsträger	Ein Praxisverbund führt eine gemeinsame Patientenkartei. Eine Betreuungseinrichtung übermittelt Bewohnerdaten an einen Apothekendienst zur Medikamentenversorgung.	4, 5
2.	Umfangreiche Verarbeitung von Daten über den Aufenthalt von Personen.	Ambulante Dienste Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren in Dienstfahrzeugen Demenzüberwachung	Ein Dienstleister erfasst die Standorte, Fahrstrecken und Verweilzeiten der Mitarbeiter um daraus eine Routenoptimierung zu errechnen. Ein Unternehmen erhebt Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren. Eine Betreuungseinrichtung erfasst laufend den Aufenthalt von Bewohnern mit Weglauftendenz.	3, 5, 8 5, 8 3. 7

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
3.	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern ▪ die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, ▪ für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, ▪ die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und ▪ der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können.	Verknüpfung von Beratungsangeboten	Eine Beratungsstelle gleicht die erhobenen Daten aus verschiedenen Beratungsangeboten (z.B. Suchthilfe und Schuldnerberatung) ohne das Wissen der Betroffenen miteinander ab, um zusätzliche Beratungsansätze zu finden.	2, 4, 6, 8
		Fundraising	Caritative Organisationen nutzen nicht selbst erhobene Daten um die Betroffenen um eine Spende zu bitten	5, 6

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
4.	Verarbeitung von Daten gemäß §§ 11 und 12 KDG durch Auftragsverarbeiter, denen von einem Gericht oder einer Verwaltungsbehörde eines Drittlands die Pflicht auferlegt werden kann, diese Daten entgegen Art. 48 DSGVO zu exportieren oder offenzulegen.	Einsatz von Dienstleistern mit Sitz außerhalb der EU durch pädagogische Einrichtungen Medizinische Leistungserbringer	Datenverarbeitung von personenbezogenen Schülerdaten gemäß Art. 11 KDG in einer öffentlichen Cloud (z. B. in einem digitalen Klassenbuch – Dokumentation von Fehlzeiten, Entschuldigungen oder anderen Dokumentationen) Abwicklung einer TeleSprechstunde mit Daten- oder Dokumentenübertragung	4, 6, 8
5.	Mobile und für die Betroffenen intransparente optoelektronische Erfassung öffentlicher Bereich	Einsatz mobiler Videotechnik Fahrzeugdatenverarbeitung – Umgebungssensoren	Ein ambulanter Dienst rüstet seine Mitarbeiter mit Videokameras aus, um diese bei der Dokumentation ihrer Tätigkeiten zu unterstützen. Ein Unternehmen erhebt Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.	3, 7, 8 3, 5, 8

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
6.	Erfassung und Veröffentlichung von Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen.	Betrieb von Bewertungsportalen	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Online-Bewertungsportal bspw. für Ärzte, Pfleger, Selbstständige oder Lehrer.	1, 6, 9

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
7.	Verarbeitung von umfangreichen Angaben über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben, oder diese in andere Weise erheblich beeinträchtigen.	Einsatz von Data-LossPrevention Systemen, die systematische Profile der Mitarbeiter erzeugen Geolokalisierung von Beschäftigten	Zentrale Aufzeichnung des Internetverlaufs und der Aktivitäten am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen. Eine Einrichtung lässt Bewegungsprofile von Beschäftigen erstellen (per RFID, Handy-Ortung oder GPS) zur Sicherung des Personals (Rettungsdienst, Ersthelfer), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (LKW mit Ladung) oder zur Überwachung kritischer Zeitabläufe (Transport von Blutkonserven, Spenderorganen) oder zur Koordination/Optimierung von Arbeitseinsätzen im Außendienst.	3, 4, 5, 8

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
8.	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten, sofern ▪ die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, ▪ für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, ▪ die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und ▪ der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen.	Big-Data-Analyse von Kunden- und sonstigen personenbez. Daten, die mit Angaben aus Drittquellen angereichert wurden.	Quartiersanalyse: In einem größeren Wohngebiet werden die Daten von Wohnungsgesellschaften, Meldebehörden, Einzelhändlern, sozialen Diensten etc. zusammengeführt, um kommunalen Handlungsbedarf zu ermitteln .	1, 5, 6
9.	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	Telefongespräch-Auswertung mittels Algorithmen	Die Telefonseelsorge ermittelt mit Hilfe einer Stimmfrequenzanalyse die Stimmungslage des Anrufers.	1, 3, 4, 8

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
10.	Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen.	Erfassung des Kauf- oder Freizeitverhaltens unterschiedlicher Personenkreise zur Profilbildung und Kundenbindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten.	Ein Verbund sozialer Einrichtungen gibt eine „Ehrenamtskarte“ aus, mit der Vergünstigungen in öffentlichen Freizeiteinrichtungen und bei bestimmten Einkaufsmöglichkeiten verbunden sind.	3, 5
11.	Anonymisierung von besonderen personenbezogenen Daten nach § 11 KDG, falls diese (ggf. vermeintlich) anonymen Daten an Dritte weitergegeben oder zu nicht nur internen statistischen Zwecken verarbeitet werden sollen. Risiko: Beim Dritten können Daten aus anderen Quellen vorliegen, durch deren Verknüpfung die Anonymisierung aufgehoben werden könnte.	Weitergabe von anonymisierten Daten an einen Dachverband	Eine Beratungsstelle gibt anonymisierte Daten über Klienten zwecks statistischer Auswertung an einen Dachverband. Dort liegen auch Daten anderer Stellen vor, die durch eine Verknüpfung Rückschlüsse auf die vermeintlich anonymisierten Daten erlauben.	4, 6

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
12.	Verarbeitung von Daten gemäß §§ 11 und 12 KDG - auch wenn sie nicht als „umfangreich“ im Sinne des § 35 Abs. 4 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von TelemedizinLösungen zur detaillierten Bearbeitung von Krankheitsdaten Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind	Ein Arzt nutzt ein Webportal oder bietet eine App an, um Patienten detailliert und systematisch zu behandeln. Eine Einrichtung organisiert und bewirbt ein Fitnessprogramm, bei dem die sportlichen Aktivitäten der Mitarbeiter über ein Fitnessarmband erfasst, zentral ausgewertet und gegen ein Ziel gemessen werden.	4, 8 1, 2, 3, 4
13.	Verarbeitung von Daten gemäß §§ 11 und 12 KDG - auch wenn sie nicht als „umfangreich“ im Sinne des § 35 Abs. 4 lit. b) anzusehen ist - sofern die Daten dazu verwendet werden, die Leistungsfähigkeit von Beschäftigten zu bestimmen	Erfassung von Leistungsdaten in medizinischen oder pflegerischen Berufen	Ein ambulanter Dienst setzt eine minutengenaue elektronische Leistungserfassung an.	1, 3, 8
14.	Verarbeitung von Daten der Personenstands- und Melderegister sowie anderer Stellen, die Daten aus diesen Registern in großem Umfang oder Meldedaten mit Sperrvermerken gemäß § 51 Abs. 1 und 5 Bundesmeldegesetz verarbeiten	Pfarramtlicher Bereich	Ein Pfarramt nutzt Meldedaten zur Durchführung einer Werbeaktion für kirchliche Vereine.	4, 5

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
15.	Umfangreiche Verarbeitung von Daten über Kinder	Schulsozialarbeit	Ein Caritas-Verband wird mit der Über-Mittag- und Hausaufgabenbetreuung von Schülern eines Schulzentrums beauftragt. Dazu werden umfangreiche Schülerdaten übergeben.	4, 5, 7
		Kinderheime	Der Betreiber eines Kindererholungsheims plant ein neues IT-System zur Verwaltung und Abrechnung der Aufenthalte.	5, 7

6.11 Rechtliche Qualität der Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 26. Juli 2018)

Nach § 44 Abs. 3 lit. f) KDG gehört es zu den Aufgaben des Diözesandatenschutzbeauftragten, „mit anderen Datenschutzaufsichten zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes zu gewährleisten."

Vor diesem Hintergrund treffen sich die Diözesandatenschutzbeauftragten in regelmäßigen Abständen, um die einheitliche Anwendung des KDG sicherzustellen.

Die Konferenz der Diözesandatenschutzbeauftragten stellt daher fest, dass die Beschlüsse der Konferenz die Rechtsauffassung der Diözesandatenschutzbeauftragten wiedergeben.

6.12 Veröffentlichung von Ehe- und Altersjubiläen, Priesterjubiläen in Presseerzeugnissen des Bistums oder der Pfarrei

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 26. Juli 2018)

Die Konferenz der Diözesandatenschutzbeauftragten spricht die Empfehlung aus, dass die (Erz-)Bistümer eine einheitliche Jubiläumsordnung erlassen.

Anmerkung:
Eine solche Jubiläumsordnung ist bereits in den Bistümern Dresden-Meißen, Erfurt, Magdeburg und Görlitz in Kraft gesetzt. Für die in Nordrhein-Westfalen belegenen (Erz-) Bistümern ist eine Regelung für den pfarramtlichen Bereich in Kraft gesetzt, die Regelungen zur Veröffentlichung von Jubiläen enthält.

„Jubiläumsordnung zur Veröffentlichung Alters- und Ehejubiläen, Geburten, Sterbefällen, Ordens- und Priesterjubiläen"

Bei Alters- und Ehejubiläen, Geburten, Ordens- und Priesterjubiläen können Namen der betroffenen Person und ggf. deren Wohnort (nicht die Straße) sowie der Tag und die Art des Ereignisses in den Publikationsorganen der Pfarreien (Pfarrnachrichten) sowie in den kircheneigenen Printmedien veröffentlicht werden.

Die betroffene Person hat das Recht, jederzeit gegen die Veröffentlichung nach Satz 1 Widerspruch einzulegen. Der Widerspruch ist

schriftlich oder in sonstiger geeigneter Form bei der zuständigen Pfarrei oder der Meldestelle des Bistums einzureichen. Diese und ggf. andere Sperrvermerke sind zu beachten.

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

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

Soll eine weitere, über die genannten Medien hinausgehende Veröffentlichung erfolgen, ist eine gesonderte Einwilligung entsprechend den Regelungen des Gesetzes über den Kirchlichen Datenschutz (KDG) einzuholen. Dies betrifft insbesondere eine Veröffentlichung im Internet.

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

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

6.13 Umgang mit dem EuGH Urteil vom 05.06.2018 über Facebook-Fanpages

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 26. Juli 2018)

Die Konferenz der Diözesandatenschutzbeauftragten weist darauf hin, dass das Urteil des Europäischen Gerichtshofes vom 05.06.2018 aus für den kirchlichen Bereich Bedeutung hat, d.h Betreiber von Fanpages im kirchlichen Bereich den Rechtswirkungen des Urteils im selben Ausmaß ausgesetzt sind wie andere Einrichtungen und Unternehmen. Für die Nutzung von Facebook-Fanpages wird auch auf das von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und Länder (DSK) Gesagte hingewiesen, das in gleicher Weise gilt.

Die Konferenz der Diözesandatenschutzbeauftragten empfiehlt den kirchlichen Einrichtungen aus diesem Grund, auf das Betreiben von Facebook-Fanpages zu verzichten.

6.14 Rechtswirksamer Verzicht auf Einwilligungen bei Fotoaufnahmen

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 10. und 11. Oktober 2018)

Die Konferenz der Diözesandatenschutzbeauftragten beschließt,

1. Eine Einwilligung zur Anfertigung und Veröffentlichung von Fotos, Film und Tonaufnahmen kann auch durch den Minderjährigen erteilt werden, sobald er über die erforderliche Einsichtsfähigkeit verfügt, was regelmäßig spätestens mit der Vollendung des 16. Lebensjahres der Fall ist.

2. Zur Veröffentlichung der Aufnahmen ist zusätzlich eine Einwilligung der Sorgeberechtigten des Minderjährigen erforderlich.

3. Die Grundsätze können nicht dadurch umgangen werden, dass das Elternrecht pauschal durch Vollmacht auf Dritte übertragen oder gänzlich auf das Grundrecht auf informationelle Selbstbestimmung verzichtet wird.

Erläuterungen zum Beschluss:
Eine einheitliche Definition von Jugendlichen oder Kindern gibt es im deutschen Recht nicht. Jedoch bezeichnet das Jugendgerichtsgesetz als Jugendliche Minderjährige zwischen 14 und 18 Jahren. Wer noch nicht 14 Jahre alt ist, wird als Kind bezeichnet.[21]

Die DSGVO macht demgegenüber keine Unterscheidung zwischen Jugendlichen und Kindern. In der Verordnung wird durchgehend von Kindern gesprochen. Art 8 Abs. 1 DSGVO bringt dennoch eindeutig zum Ausdruck, dass mit dem Begriff „Kinder" alle Personen unter 18 Jahren gemeint sind. Das KDG spricht in § 8 Abs. 8 von Minderjährigen.[22] Es geht nachfolgend also um die Einwilligung von unter 18-jährigen Personen unabhängig von der Bezeichnung in den jeweiligen Normen.

Indem die DSGVO in Art. 8 und in Erwägungsgrund 65 S. 2 ausdrücklich die Möglichkeit der Einwilligung von Kindern anspricht, ist festgestellt, dass Geschäftsfähigkeit i. S. d. Bürgerlichen Gesetzbuches für die Einwilligung nicht erforderlich ist.[23]

Die DSGVO legt kein Mindestalter fest, ab dem eine Einwilligung durch einen Minderjährigen wirksam abgegeben werden kann. Lediglich in Artikel 8 Abs. 1 DSGVO, § 8 Abs. 8 KDG wird für den Fall des Angebotes von Diensten der Informationsgesellschaft das einem Kind direkt gemacht wird für die Wirksamkeit der Einwilligung ein Mindestalter von 16 Jahren gefordert.[24] Diese Altersregelung bezieht sich ausschließlich

21 § 1 Abs. 2 JGG
22 Ebenso das DSG-EKD (Datenschutzgesetz der Evangelischen Kirche) in § 12.
23 Ernst in Paal/Pauly Art. 4 Rn. 66; Schwartmann/Hilgert in Heidelberger Kommentar Art. 8 Rn. 11.
24 Nach § 12 DSG-EKD Mindestalter 14 Jahre.

auf den benannten Anwendungsbereich. Eine generelle Voraussetzung für die Einwilligungsfähigkeit von Minderjährigen ist damit nicht festgeschrieben.[25] Insoweit ist keine Änderung durch die Verordnung gegenüber der davor geltenden Richtlinie[26] für solche Sachverhalte erfolgt, die Einwilligungen in Sachverhalte außerhalb dieser Vorschrift betrifft. Wie bislang im deutschen Recht kann deshalb auch weiterhin davon ausgegangen werden, dass die Wirksamkeit der Einwilligung eines Minderjährigen von dessen Einsichtsfähigkeit abhängt,[27] also davon ob der Minderjährige psychisch und intellektuell in der Lage ist, Bedeutung und Tragweite seiner Entscheidung einzuschätzen. Diese Sichtweise wird auch durch den Erwägungsgrund 58 gestützt. Abstrakte Aussagen, wann eine Einsichtsfähigkeit gegeben ist, insbesondere die Knüpfung an ein bestimmtes Alter, scheiden also aus.[28] Bestenfalls als ein Anhaltspunkt kann ab einem Alter von 14 bis 15 Jahren in der Regel vermutet werden[29], dass die Einsichtsfähigkeit gegeben ist, was jedoch nicht von einer Einzelfallprüfung entbindet.[30] Fehlt die Einsichtsfähigkeit, bedarf es der Einwilligung der Erziehungsberechtigten, liegt Einsichtsfähigkeit vor, ist eine doppelte Einwilligung sowohl des Minderjährigen als auch der Erziehungsberechtigten erforderlich.

Das Recht auf informationelle Selbstbestimmung ist als ein an eine bestimmte Person gebundenes Recht, das wegen seines besonderen Charakters im Grundsatz weder übertragbar noch vererblich ist,[31] ein höchstpersönliches Recht. Damit muss grundsätzlich auch eine Einwilligung in Bezug auf ein solches Recht höchstpersönlich erklärt werden.[32] Ausnahme von diesem Grundsatz ist die Abgabe der Einwilligungserklärung der Sorgeberechtigten für ihr Kind.[33] Das Recht auf informationelle Selbstbestimmung ist nach der grundlegenden Entscheidung des Bundesverfassungsgerichtes zum Volkszählungsurteil selber ein Grundrecht.[34] Das Einwilligungsrecht der Eltern in dieses Grundrecht ihrer Kinder können die Eltern nur selber ausüben. Ein Verzicht darauf ist nicht möglich.[35] Eine willkürliche Übertragung dieses Rechtes an Dritte scheitert an der Höchstpersönlichkeit dieses Rechtes, bzw. daran, dass es sich hierbei um eine wesentliche Angelegenheit i. S. d. § 1687 I BGB handelt.[36] So ist insbesondere die Übertragung des Sorgerechts im Hinblick auf die Anfertigung von Bild- und Tonaufnahmen auf einen Dritten nicht möglich. Dies muss umso mehr gelten, wenn der Dritte damit eigene Interessen verfolgt. Dies dürfte bei der Anfertigung

25 Kampert in Sydow Europäische Datenschutzgrundverordnung Art. 8 RN. 7; Schwartmann/Hilgert in Heidelberger Kommentar Art. 8 Rn. 10.
26 EU DSRL 95/46/EG vom 24.10.1995.
27 Kampert in Sydow Europäische Datenschutzgrundverordnung Art. 8 RN. 7.
28 Simitis Kommentar zum BDSG § 4a Rn. 21.
29 40. TB Hessischer Datenschutzbeauftragter.
30 Ernst, DANA 2017, 14.
31 Duden Recht A-Z. Fachlexikon für Studium, Ausbildung und Beruf. 3. Aufl..
32 Simitis Kommentar zum BDSG § 4a Rn. 30; Weichert in DKWW Kommentar zum BDSG § 4a Rn. 6; Paal/Pauly Kommentar zur DSGVO Art. 4 Rn.65; 46. TB Hessischer Datenschutzbeauftragte S. 108.
33 Ernst DANA 2017, 14.
34 BVerfGE 65, 1ff.
35 Palandt Kommentar zum BGB § 1626 RN. 3.
36 So im Ergebnis auch Hoffmann, JAmt 2015, 8.

von Fotos oder Videoaufnahmen durch Kindergärten, Schulen und bei Ferienfreizeiten der Fall sein, da diese zumindest auch der Werbung für diese Einrichtung dienen. Insoweit dürfte ein Interessenkonflikt bei den Beauftragten bestehen.

Eine pauschale Generaleinwilligung für alle gleichgelagerten Fälle für die Dauer der Zugehörigkeit des Minderjährigen in einer Einrichtung ist grundsätzlich unzulässig. Dies wird insbesondere Einwilligungen zur Erstellung von Fotos und deren Veröffentlichung betreffen, die bei Aufnahme in die KITA oder die Schule für die gesamte Aufenthaltszeit erteilt werden. Art 4 Nr. 11 DSGVO wie auch § 8 Nr. 13 KDG definieren „Einwilligung" als eine Willensbekundung in informierter Weise für einen bestimmten Fall. Eine informierte Einwilligung dürfte in der pauschalen Einwilligung für die Veröffentlichung aller Fotos während der gesamten Aufenthaltsdauer kaum anzunehmen sein.[37] Außerdem kann unter einem „bestimmten Fall" nicht die Anfertigung von Fotos gemeint sein, sondern nur die Anfertigung und Veröffentlichung eines konkreten, eben bestimmten Fotos.

Eine Veröffentlichung liegt vor, wenn Daten einer nicht genau feststehenden Mehrzahl von Adressaten, die Dritte sind, zugänglich gemacht werden.[38] Sind die Personen miteinander oder mit dem Veranstalter bekannt, gehören sie nicht zur Öffentlichkeit.[39] Bei KITA´s dürfte deshalb keine Veröffentlichung darin zu sehen sein, wenn Bilder von Kindern innerhalb der Einrichtung ausgehängt werden.[40] Für diese Fälle ist von der ausnahmsweisen Zulässigkeit einer Generaleinwilligung auszugehen. Dies betrifft aber ausdrücklich nur den Innenbereich der Einrichtung im Rahmen der Zweckbindung. Aushänge in Schaukästen oder Veröffentlichung in Flyern sind von dieser Ausnahme nicht umfasst.[41] Für Schulen trifft dies nicht in gleicher Weise zu, da der Kreis der Dritten die Zugang zu der Einrichtung haben nicht wie bei Kindereinrichtungen überschaubar ist.

Ein Verzicht auf Grundrechte ist zumindest dann nicht möglich, wenn das Grundrecht über den einzelnen hinaus auch der Gemeinschaft zugutekommt. Nach Auffassung des Bundesverfassungsgerichts ist die Entfaltung der Persönlichkeit zu gewährleisten, weil Selbstbestimmung eine elementare Funktionsbestimmung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist.[42]

37 46. TB hessischer Landesbeauftragte für Datenschutz S. 109.
38 Dammann in Simitis Kommentar zum BDSG § 3 Rn. 157.
39 § 15 Abs. 3 UrhG.
40 Caritasverband für das Bistum Trier e.V. Arbeitshilfe Datenschutz in katholischen Tageseinrichtungen für Kinder.
41 Ministerium für Kultus, Jugend und Sport Baden-Württemberg Datenschutzbroschüre Datenschutz in Kindertageseinrichtungen S. 16; Gutenkunst/Fachet Merkblatt für den Datenschutz in evangelischen und katholischen Kindertageseinrichtungen S. 7.
42 BVerfGe 65, 1ff.

6.15 Nutzung von Messengerdiensten (ergänzend zum Beschluss aus Mai 2017)

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 10. und 11. Oktober 2018)

Die Konferenz der Diözesandatenschutzbeauftragten beschließt, dass die Verwendung eines Messenger-Dienstes zu dienstlichen Zwecken untersagt ist, soweit eine physikalische Datenspeicherung außerhalb des Gebietes des EWR und der Schweiz stattfindet und keine Punkt-zu-Punkt-Verschlüsselung genutzt wird. Auf den Beschluss vom 26.07.2018 (Beurteilung von Messenger- und anderen Social-Media-Diensten) wird verwiesen.

6.16 Facebook-Fanpages

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 10. und 11. Oktober 2018)

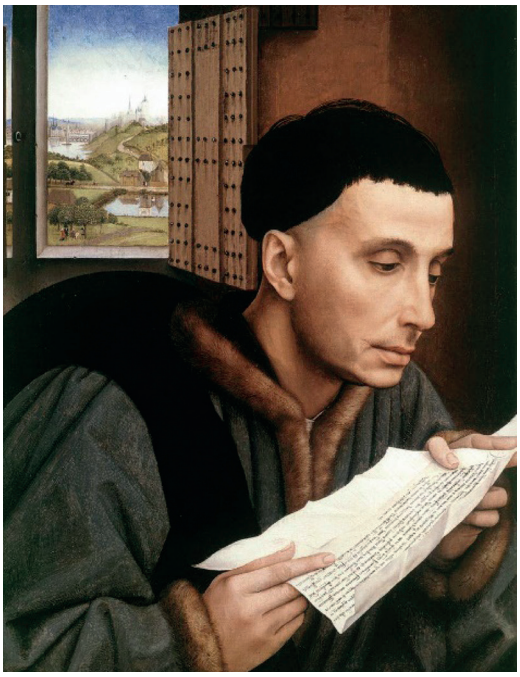
Die Konferenz der Diözesandatenschutzbeauftragten spricht erneut die Empfehlung aus, auf das Betreiben einer Facebook-Fanpage zu verzichten, da eine datenschutzrechtliche Haftung des Betreibers einer Fanpage nicht wirksam ausgeschlossen werden kann.

Dieser Beschluss knüpft an die Empfehlung der Diözesandatenschutzbeauftragten vom 26. Juli 2018 an, dass die Grundsätze der Datenschutzkonferenz des Bundes und der Länder (DSK) zum EuGH-Urteil vom 05.06.2018 ebenso für kirchliche Einrichtungen gelten, welche eine Fanpage bei Facebook betreiben. Ebenso sollten die kirchlichen Stellen den Fragenkatalog beachten, den die DSK am 05. September 2018 herausgegeben hat.

Die unmittelbar danach erfolgten Anpassungen der vertraglichen Grundlagen von Facebook zu den Insights-Daten können aus Sicht der Konferenz der Diözesandatenschutzbeauftragten die aufgeworfenen datenschutzrechtlichen Fragenstellungen nicht vollständig beantworten.

Abkürzungsverzeichnis

BAG	Bundesarbeitsgericht
bDSB	betrieblicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfD EKD	Beauftragter für den Datenschutz der EKD
BGH	Bundesgerichtshof
DDSB	Diözesandatenschutzbeauftragter
DOK	Deutsche Ordensobernkonferenz
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSG-EKD	Datenschutz der Evangelischen Kirche in Deutschland
DSGVO	Europäische Datenschutzgrundverordnung
EDPB	European Data Protection Board (dt. EDSA)
EDSA	Europäischer Datenschutzausschuss (engl. EDPB)
EKD	Evangelische Kirche in Deutschland
ENISA	Agentur der Europäischen Union für Netz- und Informationssicherheit
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
ITSVO-EKD	IT-Sicherheitsverordnung EKD
KDG	Gesetz über den Kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz
KDO	Anordnung über den kirchlichen Datenschutz
KDO-DVO	Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz
KDSGO	Kirchliche Datenschutzgerichtsordnung
KDSZ	Katholisches Datenschutzzentrum
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturhebergesetz)
LfD	Landesbeauftragter für den Datenschutz
LDI	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
NRWDSAnpUG-EU	Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU
VDD	Verband der Diözesen Deutschlands
VwVfG	Verwaltungsverfahrensgesetz



Hl. Ivo

Der heilige Ivo ist der Schutzpatron des Katholischen Datenschutzzentrums.
Er lebte im 13. Jahrhundert im heutigen Frankreich und setzte sich dort unter anderem für Arme und Bedrängte vor weltlichen und kirchlichen Gerichten ein.
Das Bildnis des heiligen Ivo ziert auch das Siegel des katholischen Datenschutzzentrums. Sein Gedenktag ist der 19. Mai.

Quelle Foto: Joachim Schäfer – www.heiligenlexikon.de

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de