Jahresbericht 2019

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.–31.12.2019

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
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

4. 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 01.01.2019– 31.12.2019

Redaktionsschluss: 30. Juni 2020

Inhaltsverzeichnis

Vorwort

In ihrem Gemeinsamen Wort „Vertrauen in die Demokratie stärken“ vom 11. April 2019 gehen die Deutsche Bischofskonferenz und der Rat der Evangelischen Kirche in Deutschland auch auf die Bedeutung des Datenschutzes für die Demokratie ein. Sie stellen dazu fest: „Unter den Bedingungen von ‘‘Big Data‘‘ ist der Datenschutz zu einer zentralen politischen Aufgabe geworden. Wichtig ist ein starker gesetzlich verankerter Datenschutz, ebenso aber der sorgsame und verantwortliche Selbstschutz im Umgang mit den eigenen Daten“ (Abschnitt 4.4 des Gemeinsamen Wortes).

„Wichtig ist … der sorgsame und verantwortliche Selbstschutz im Umgang mit den eigenen Daten.“

Die katholische Kirche hat mit dem Gesetz über den Kirchlichen Datenschutz (KDG) in Anlehnung an die Europäische Datenschutz-Grundverordnung (DSGVO) eine solche starke gesetzlich verankerte Grundlage für den Datenschutz in kirchlichen Stellen und Einrichtungen geschaffen.

Gleichzeitig wirbt das Katholische Datenschutzzentrum für die Wahrnehmung der eigenen Verantwortung im Umgang mit den persönlichen Daten. Wir wollen die Menschen, deren personenbezogene Daten verarbeitet werden, mit verschiedenen Informationsangeboten erreichen und sensibilisieren. Ebenso wichtig ist aus Sicht des Katholischen Datenschutzzentrums die Sensibilisierung derjenigen Stellen, die die Daten verarbeiten.

Die Verunsicherungen und die Aufregung bei den kirchlichen Einrichtungen, die sich im Zuge der Einführung des neuen Gesetzes im Mai 2018 ergeben hatten, sind einer stetigen Beschäftigung mit den bestehenden und neuen Herausforderungen des kirchlichen Datenschutzgesetzes gewichen. Im Berichtszeitraum konnten viele Fragen beantwortet und Lösungen für große und kleine Probleme gefunden werden.

Diese - im positiven Sinne - dauerhafte Beschäftigung mit dem Thema Datenschutz und der damit verbundenen stetigen Suche nach den passenden Lösungen sowie dem Ringen um den bestmöglichen Ansatz zur Umsetzung der gesetzlichen Forderungen, ist für die starke Verankerung des Datenschutzes aber ebenso entscheidend wie ein starkes Gesetz.

Nur der immer wieder neu gefasste Entschluss, die Anforderungen des Gesetzes bei der Arbeit mit den Daten der Gläubigen, Patienten, Bewohner, Hilfesuchenden, Kunden oder Beschäftigten umfassend und bestmöglich umzusetzen, ermöglicht den notwendigen Schutz der Menschen. Denn Datenschutz schützt keine Daten. Es schützt die Menschen, deren Daten verarbeitet werden.

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

1 Entwicklungen im Datenschutzrecht

Auch im Jahr 2019 entwickelten sich die datenschutzrechtlichen Regelungen auf allen Ebenen weiter, sowohl auf europäischer Ebene, auf Bundes- und Landesebene und in der Kirche.

Dabei gab es neben neuen Regelungen der Gesetzgeber auf den verschiedenen Ebenen auch zunehmend Auslegungen des geltenden Rechts durch den Europäische Datenschutzausschuss, die Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder und die Konferenz der Diözesandatenschutzbeauftragten (DDSB).

1.1 Gesetzgeberische Entwicklungen auf Ebene der Europäischen Union

Auf europäischer Ebene wurde im Berichtszeitraum weiterhin um die Verabschiedung der e-Privacy-Verordnung gerungen. Diese sollte ursprünglich parallel zur Datenschutz-Grundverordnung 2018 in Kraft treten. Daneben gab es auch noch weitere, datenschutzrechtlich relevante Gesetzgebungsvorhaben auf europäischer Ebene.

1.1.1 e-Privacy-Verordnung – Quo vadis?

Der Entwurf der e-Privacy-Verordnung („Verordnung des Europäischen Parlaments und des Rates 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)")[1] stellt eine Initiative auf Ebene der Europäischen Union (EU) dar, mittels der neue Rahmenbedingungen für digitale Kommunikationsmöglichkeiten zur Stärkung des digitalen Binnenmarktes geschaffen werden sollen. Dabei beabsichtigt die EU gleichermaßen, die Privatsphäre von Bürgern online zu stärken und den Datenschutz intensiver zu regulieren, verbunden mit einer möglichen Stärkung des digitalen Binnenmarktes.

Diese neue e-Privacy-Verordnung sollte ursprünglich im Mai 2018 in Kraft treten, parallel zur Anwendbarkeit der DSGVO, um so für die jeweiligen Regelungsbereiche aktuelle, sich ergänzende Vorgaben machen zu können. 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.

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

1 Entwurf der Europäischen Kommission vom 10.02.2017, COM (2017) 10.

1.1.2 EU-Verordnung zur Cybersicherheit

Die EU-Verordnung zur Cybersicherheit (Verordnung (EU) 2019/881 vom 17. April 2019) fasst zum einen die Aufgaben und die Ausstattung der Agentur der Europäischen Union für Cybersicherheit (ENISA) neu, die mit den Mitgliedstaaten und dem privaten Sektor auf dem Gebiet der Cybersicherheit zusammenarbeitet und auf europäischer Ebene Strategien zur Computer- und Netzsicherheit entwirft. Weiterhin wird mit der Verordnung ein EU-weiter Rahmen für die IT-Sicherheitszertifizierungen von Produkten, Dienstleistungen und Prozessen geschaffen.

Ein wichtiges Ziel der Verordnung ist eine weitere Stärkung der Sicherheit in der Europäischen Union im Bereich des Internets und der Cyberaktivitäten. Als weiterer Effekt wird eine größere Rechtssicherheit für europaweit tätige Unternehmen sowie auch für die Verbraucher geschaffen. Die bereits durch die Europäische Datenschutz-Grundverordnung geforderten Prinzipien, durch nutzerfreundliche Voreinstellungen und Design Datenschutz zu gewährleisten, werden hier für den Bereich der Cybersicherheit vorgegeben.

1.1.3 EU-Richtlinie zum Schutz von Personen, die Verstöße melden

Die Thematik von Hinweisgebern beziehungsweise „Whistleblowern" hat aufgrund einiger spektakulärer Fälle mediale Aufmerksamkeit erfahren. Dabei war jedoch nicht immer geklärt, ob und in welchem Umfang sich die Hinweisgeber in einem gesetzlich zulässigen Rahmen bewegen. Der Bedarf an klarstellenden Regelungen und möglichst eindeutigen gesetzlichen Vorgaben ist dabei deutlich geworden. Ebenso zeigte sich die Notwendigkeit, den Umfang eines Schutzbedarfs von Hinweisgebern zu definieren. Hinweisgeber müssen in die Lage versetzt werden, risikolos auf ungesetzliche Zustände hinzuweisen, damit sie die vom Gesetzgeber gewünschten und erforderlichen Hinweise nicht unterlassen. Ohne gesetzlichen Schutz müssen Hinweisgeber mit negativen Konsequenzen rechnen, darunter auch mit dem Verlust ihres Arbeitsplatzes oder mit persönlichen Repressionen.

„Hinweisgeber müssen in die Lage versetzt werden, risikolos auf ungesetzliche Zustände hinzuweisen …"

Mit der Richtlinie (EU) 2019/1937 vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, soll diesen Zielen Rechnung getragen werden. Auch wird über die Regelung als EU-Richtlinie eine Vorgabe geschaffen, die dann möglichst europaweit einheitlich Geltung erlangen und Mindeststandards setzen kann. Dadurch wird vermieden, dass in den EU-Mitgliedstaaten ein unterschiedliches Niveau bezüglich der Umgangsweise mit und der Betrachtung von Hinweisgebern besteht. Die Richtlinie kann Vorgaben für sichere Kanäle für die Meldung von Missständen sowohl innerhalb einer Organisation als auch an und gegenüber Behörden schaffen. Darüber hinaus werden Hinweisgeber vor Kündigungen, Zurückstufungen und anderen Repressalien geschützt. Nationale Behörden werden verpflichtet, die Bürger zu informieren und öffentliche Stellen im Umgang mit Hinweisgebern zu schulen.

Betroffen sind unter anderem die Meldung von Verstößen gegen das EU-Recht in den Bereichen öffentliche Auftragsvergabe,

Finanzdienstleistungen, Geldwäsche und Terrorismusfinanzierung, Produktsicherheit, Verkehrssicherheit, Umweltschutz, kerntechnische Sicherheit, Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz, öffentliche Gesundheit, Verbraucherschutz, Schutz der Privatsphäre, Datenschutz und Sicherheit von Netz- und Informationssystemen. Die neuen Vorschriften sollen außerdem bei Verstößen gegen die EU-Wettbewerbsvorschriften und die Körperschaftsteuer-Vorschriften sowie bei Schädigungen der finanziellen Interessen der EU zur Anwendung kommen. Die Kommission empfiehlt dabei den Mitgliedstaaten, über diese Mindeststandards hinauszugehen und darauf aufbauend umfassende Rahmenbedingungen für den Schutz von Hinweisgebern zu schaffen. Insoweit ist auch noch abzuwarten, welche konkreten Regelungen der Bundesgesetzgeber vorsehen wird und ob er den Schutz auch auf die Meldung von Verstößen gegen nationales Recht ausdehnt.

Zum Schutz des Hinweisgebers sieht die Richtlinie z.B. in ihrem Art. 19 das Verbot von Repressalien vor. Die verschiedenen Arten von Repressalien werden ausdrücklich aufgeführt, wie etwa die Suspendierung, Entlassung oder Degradierung. Zum weitergehenden Schutz ist geregelt, dass bei dennoch erlittenen Repressalien ein Anspruch auf Entschädigung besteht. Gemäß Art. 24 können die Schutzmaßnahmen der Verordnung nicht individualrechtlich, z. B. in einem Arbeitsvertrag, abbedungen werden. Unter bestimmten Voraussetzungen darf sich der Hinweisgeber bei vorheriger erfolgloser anderweitiger Informationsweitergabe (z. B. an interne Stellen oder an Behörden) auch an die Öffentlichkeit wenden. Dies ist dann erlaubt, wenn die Hinweisgeber im privaten oder öffentlichen Sektor tätig sind und es sich um Informationen handelt, die sie in ihrem beruflichen Tätigkeitsfeld erlangt haben. Der Schutz erstreckt sich unter Umständen auch auf Dritte, die mit dem Hinweisgeber in Verbindung stehen.

Die Richtlinie führt bezüglich der Nachweisbarkeit von Repressalien zu einer Beweislastverteilung zulasten des Arbeitgebers beziehungsweise desjenigen, der die Benachteiligung zu verantworten hat. Der benachteiligte Hinweisgeber muss nicht nachweisen, dass eine Repressalie aufgrund seiner Funktion als Whistleblower erfolgt ist, sondern der Verantwortliche muss darlegen und begründen, dass z.B. eine ausgebliebene Beförderung nicht damit in einem engen Zusammenhang steht.

Allerdings ist zu beachten, dass der Hinweisgeber dann nicht geschützt wird, wenn das Beschaffen der Informationen nur mittels der Begehung einer Straftat möglich ist.

Neu ist, dass für juristische Personen ab einer bestimmten Betriebsgröße Meldekanäle eingerichtet werden sollen. Interne Meldekanäle werden auch für die juristischen Personen des öffentlichen Sektors gefordert. Die Richtlinie enthält Vorgaben, wie diese Meldekanäle ausgestaltet werden sollen, wozu auch Meldewege, der Umgang mit der Meldung und deren Dokumentation gehören.

Die Umsetzung der Richtlinie in das jeweilige nationale Recht soll durch die Mitgliedstaaten bis zum 17. Dezember 2021 erfolgen.

1.1.4 Brexit

In einem Referendum hatte das Vereinigte Königreich von Großbritannien und Nordirland bereits am 26. Juni 2016 für den Austritt aus der EU gestimmt. Nach mehreren Verschiebungen hat dieser Austritt mit Wirkung zum 31. Januar 2020 stattgefunden.

Seit dem 31.01.2020 läuft eine Übergangsphase bis Jahresende 2020, in der die Vertreter der EU und der britischen Regierung über die Ausgestaltung des künftigen Verhältnisses miteinander sowie der dann geltenden Rechtsgrundlagen verhandeln werden. Das Ergebnis dieser Beratungen ist in Anbetracht der bisher bekannt gegebenen unterschiedlichen Auffassung nur schwer vorherzusehen.

Der Austritt des Vereinigten Königsreichs aus der EU wird zunächst zur Folge haben, dass Großbritannien im Sinne des Datenschutzes zu einem Drittland außerhalb der EU wird. Die Folgen dieses Status werden in einem Abkommen festgelegt werden müssen, das die Details der künftigen Beziehungen und der Anwendung der Rechtsregeln im Verhältnis zueinander festlegt. Davon wird auch der Bereich des Datenschutzes betroffen sein, wobei für die Übergangsphase die DSGVO zunächst weiter gelten wird. Dies vorausgesetzt wird sich folglich für den Austausch personenbezogener Daten und den Einsatz britischer Systeme, Produkte und Angebote bis zum Jahresende 2020 nichts ändern. Es wird daher zu beobachten sein, welche Ergebnisse bezüglich des Datenschutzes und der anzuwenden Rechtsregelungen in den künftigen Verhandlungen für die Zeit ab 2021 erzielt werden.

Sollte noch während der Übergangszeit das anzuwendende Datenschutzrecht von Seiten Großbritanniens geändert werden, wird die Reaktion der zuständigen Stellen der EU abzuwarten sein. Dies kann möglicherweise Auswirkungen auf die Nutzung britischer Systeme, Produkte und Angebote haben.

Die kirchlichen Stellen sollten darauf vorbereitet sein, dass sich die datenschutzrechtlichen Bedingungen für die Verarbeitung personenbezogener Daten unter Beteiligung von Stellen mit Sitz in Großbritannien zum Jahreswechsel 2020/2021 ändern werden und ihre Prozesse und Datenflüsse sowie die entsprechenden Verträge überprüfen und gegebenenfalls kurzfristig ändern.

1.2 Gesetzgeberische Entwicklungen in der Bundesrepublik Deutschland

Auf Bundesebene wurde im Berichtszeitraum vor allem mit dem zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) die Anpassung der deutschen Gesetze an die Vorgaben der DSGVO und der JI-Richtlinie zum Datenschutz fortgeführt. Daneben gab es auch noch weitere, datenschutzrechtlich relevante Gesetzgebungsvorhaben auf nationaler Ebene.

1.2.1 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU

Mit dem ersten Datenschutz-Anpassungs- und Umsetzungsgesetz EU hatte der deutsche Bundesgesetzgeber bereits in sehr grundlegender Weise das deutsche Datenschutzrecht auf Bundesebene überarbeitet. Das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU) enthielt vor allem ein neues Bundesdatenschutzgesetz (BDSG). Schon vor der Verabschiedung dieses Gesetzes hatte sich jedoch gezeigt, dass auch notwendiger Änderungsbedarf an vielen anderen Bundesgesetzen bestand, der in dem vorgegebenen Zeitrahmen noch nicht in dieses Gesetzespaket gepackt werden konnte. Zur Realisierung dieser Überlegungen wurde das zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU erarbeitet und verabschiedet.

Mit diesem zweiten Gesetzespaket zur Anpassung nationaler Regelungen an europäisches Datenschutzrecht wurden auch Änderungen am BDSG vorgenommen. Eine viel diskutierte Änderung bewirkt Art. 12 Nr. 9 dieses Gesetzes mit der Erhöhung des Wertes „10“ auf „20“ in § 38 Abs. 1 BDSG betreffend die Verpflichtung zur Benennung eines betrieblichen Datenschutzbeauftragten. Damit werden kleinere Unternehmen, welche den neuen Grenzwert unterschreiten, nicht mehr der Verpflichtung unterworfen, einen eigenen Datenschutzbeauftragten zu benennen. Dies ist zwar auch als Teil einer Bürokratieerleichterung betrachtet worden, bedeutet andererseits aber eine Schwächung des Bestrebens, einen möglichst umfassenden und qualifizierten Datenschutz in den Einrichtungen sicherzustellen. Darüber hinaus sollten sich die Verantwortlichen, die nunmehr keinen betrieblichen Datenschutzbeauftragten mehr benennen müssen, nicht der Illusion erleichterter Rahmenbedingungen hingeben. Denn die gesetzlichen Anforderungen an die eigene Datenverarbeitung ändern sich durch eine nicht mehr bestehende Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten nicht und die Verantwortung bleibt bei den Leitungen der Einrichtungen. Ihnen fehlt aber zukünftig der fachkundige datenschutzrechtliche Berater, den sie ansonsten im Rahmen ihrer Entscheidungsprozesse hätten hinzuziehen können.

Das derzeitige kirchliche Recht stellt in § 36 Abs. 2 lit. a) des Gesetzes über den Kirchlichen Datenschutz darauf ab, dass „sich bei ihnen (d. h. bei kirchlichen Stellen) in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen“. Es bleibt abzuwarten, wie der kirchliche Gesetzgeber auf die Änderungen im Bundesrecht reagiert.

1.2.2 Gesetz zum Schutz von Geschäftsgeheimnissen

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)[2] dient dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung (§ 1 Abs. 1 GeschGehG). Mit dem Gesetz wird die Richtlinie (EU) 2016/943 zum Schutz von Geschäfts-

2 Art. 1 des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung vom 18. April 2019.

geheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung in deutsches Recht übertragen.

Das Gesetz hat zum Ziel, Unternehmen besser vor Spionage, auch durch Wettbewerber, zu schützen. Andererseits sollen Journalisten und ihre Hinweisgeber, die Verstöße gegen Gesetze oder Missstände aufdecken, geschützt werden. Somit bewirkt dieses Gesetz auch einen Schutz von Whistleblowern.

Als geschützte Geheimnisse gelten Geschäftsgeheimnisse, welche unter anderem durch eine eigenständige Entdeckung oder eine eigenständige Schöpfung entstanden sind. Der Begriff des Geschäftsgeheimnisses, der bisher durch Entscheidungen der Gerichte ausgestaltet worden war, wird erstmalig gesetzlich definiert und darüber hinaus europaweit einheitlich formuliert.

Die zugrunde liegende europäische Richtlinie zielt dabei auf einen einheitlichen Mindeststandard für den Schutz von Geschäftsgeheimnissen ab. In der weiteren Konsequenz können die Betroffenen verlangen, dass dem Verletzenden zugänglich gemachte Dokumente, elektronische Dateien oder Gegenstände vernichtet beziehungsweise herausgegeben werden. Auf Basis der Geheimnisverletzung erstellte Produkte können zurückgerufen oder zerstört werden. Zudem können die Betroffenen Ansprüche auf Beseitigung der Beeinträchtigung und auf Unterlassung bei drohender Wiederholungsgefahr geltend machen. Verbunden damit sind ein Auskunftsanspruch sowie das Recht auf Schadensersatz.

Das Bestehen eines Geschäftsgeheimnisses erfordert, dass der Betroffene angemessene Maßnahmen zum Schutz seiner Geheimnisse trifft. Dazu gehören sowohl physische Zugangsbeschränkungen, als auch vertragliche Sicherungsmechanismen. Erforderlich ist darüber hinaus ein berechtigtes Interesse am Schutz der Informationen, die das Geschäftsgeheimnis bilden. Dabei kann jedes von der Rechtsordnung gebilligte Interesse laut der Gesetzesbegründung ein solches berechtigtes Interesse darstellen und kann Interessen wirtschaftlicher oder ideeller Art umfassen.

Zu beachten ist, dass es für Journalisten und Whistleblower einen Ausnahmetatbestand gibt, bei dem zu prüfen ist, ob ihr jeweiliges Handeln darunter gefasst werden kann.

1.3 Gesetzgeberische Entwicklungen in der römisch-katholischen Kirche

Im kirchlichen Bereich sind im Berichtszeitraum ebenfalls neue Regelungen in Kraft getreten oder verabschiedet worden, die datenschutzrechtliche Vorgaben enthalten.

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

Mit der am 19. November 2018 von der Vollversammlung der Deutschen Bischofskonferenz verabschiedeten Durchführungsverordnung[3] hat die katholische Kirche für den Bereich des kirchlichen Datenschutzes das KDG erläuternde und präzisierende weitere Regelungen getroffen. Diese Ausführungsbestimmung ist in den (Erz-)Diözesen mit Wirkung zum 01. März 2019 und für den Verband der Diözesen Deutschland (VDD) mit Wirkung zum 01.07.2019 in Kraft getreten. Die Gesetzgeber in der katholischen Kirche haben sich in Konkretisierungen und Klarstellungen detaillierter zu den datenschutzrechtlichen Vorgaben für die dem KDG unterfallenden kirchlichen Stellen geäußert. Eine vergleichbare Regelung hatte mit der zur Anordnung über den kirchlichen Datenschutz (KDO) erlassenen Durchführungsverordnung bereits bestanden.

Die neue Durchführungsverordnung führt die bereits bekannten Vorgaben aus der bisherigen Durchführungsverordnung zur KDO fort und passt sie den Anforderungen des KDG an. Das grundlegende System ist schon durch die Vorläuferregelung vertraut. Die KDG-DVO enthält daher grundsätzlich keine großen Überraschungen für die Anwender. Sie formuliert aber an einigen Stellen die umzusetzenden Inhalte klarer. Dazu gehört unter anderem, dass sich Verantwortliche im Rahmen ihrer Verantwortung Gedanken darüber machen müssen, welche Qualität die von ihren Stellen verarbeiteten personenbezogenen Daten besitzen. Dies hat – wie schon nach der bisherigen KDO-DVO - zur Folge, dass z. B. Daten in die nach der Durchführungsverordnung vorgesehenen Kategorien einzuordnen sind. Je nach Art der Einordnung und der Schutzbedürftigkeit der personenbezogenen Daten sind entsprechende Schutzmaßnahmen zu treffen.

Das Katholische Datenschutzzentrum wird bei zukünftigen Prüfungen auch die Umsetzung der Durchführungsverordnung mit in den Blick nehmen. Die kirchlichen Einrichtungen sollten daher ihre Datenverarbeitungen und Prozesse daraufhin überprüfen, ob diese auch den Vorgaben der KDG-DVO entsprechen.

1.3.2 Ordnung und Rahmenordnung zum Schutz vor sexuellem Missbrauch

Die Deutsche Bischofskonferenz hat mit der „Ordnung für den Umgang mit sexuellem Missbrauch Minderjähriger und schutz- oder hilfebedürftiger Erwachsener durch Kleriker und sonstige Beschäftigte im kirchlichen Dienst – ehemals Leitlinien“ und der „Rahmenordnung – Prävention gegen sexualisierte Gewalt an Minderjährigen und schutz- oder hilfebedürftigen Erwachsenen im Bereich der Deutschen Bischofskonferenz“ die kirchlichen Regelungen zur Verhinderung von Fällen sexuellen Missbrauchs und zur Aufarbeitung von Missbrauchsfällen überarbeitet. Die neuen Regelungen sind in den (Erz-)Diözesen zum 01.01.2020 in Kraft getreten.

3 Siehe auch die Ausführungen im Jahresbericht 2018 des Katholischen Datenschutzzentrums, Abschnitt 1.3.3.

Bei der Aufarbeitung von Missbrauchsfällen werden sehr sensible personenbezogene Daten der Opfer, aber auch der Beschuldigten verarbeitet. Die Regelungen enthalten Vorgaben zum Umgang mit diesen Daten. Dabei kann und soll der Datenschutz die Aufklärung der Vorwürfe nicht verhindern. Die in den beiden Regelwerken enthaltenen Vorgaben zum Datenschutz sollen im Verfahren die Rechte aller Beteiligten im erforderlichen Umfang schützen helfen, ohne auf die Aufklärung Einfluss zu nehmen.

1.3.3 Weitere Gesetzgebungsvorhaben mit datenschutzrechtlichen Regelungen in der katholischen Kirche

Wie schon im Jahresbericht 2018 beschrieben, wird in der katholischen Kirche an einer möglichen Nachfolgeregelung für die aktuell in einzelnen (Erz-)Diözesen bestehenden Patientendatenschutzordnungen gearbeitet. Beabsichtigt ist, eine Vorlage für die diözesane Gesetzgebung zu schaffen, die zu einer möglichst einheitlichen bundesweiten Rechtsanwendung im Bereich des Patientendatenschutzes führen kann. Für diese Gesetzesmaterie bleibt abzuwarten, welche bereichsspezifischen Regelungen getroffen werden.

Einzelne (Erz-)Diözesen in der katholischen Kirche haben in der Vergangenheit Ausführungsbestimmungen im Sinne des § 56 KDG getroffen. Zum Teil ist die Geltung dieser Regelungen im Rahmen der Übergangsbestimmungen gemäß § 57 KDG verlängert worden. Sofern Altregelungen noch nicht an die neue Rechtslage angepasst worden sind, sind sie gemäß § 57 Abs. 5 KDG nur insoweit weiter anwendbar, wie sie den Regelungen des KDG nicht entgegenstehen. Möglicherweise sind von den (Erz-)Diözesen Anpassungen dieser Bestimmungen an die neuen Vorgaben des KDG oder neue Gesetze und Ausführungsbestimmungen zu erwarten.

1.4 Gesetzgeberische Entwicklungen in der Evangelischen Kirche in Deutschland (EKD)

Im Berichtszeitraum hat die EKD als solche keine weiteren eigenständigen Datenschutzregelungen getroffen. In den verschiedenen Landeskirchen sind jedoch landesspezifische Ausführungsbestimmungen erlassen worden. In diesen werden zum Teil spezielle Aufgabenzuweisungen geregelt, wie etwa in der bremischen Landeskirche zu Kompetenzen des Kirchenausschusses. Dieser soll die Möglichkeit erhalten, gegebenenfalls die in dem entsprechenden Gesetz vorgesehene Zuweisung der Datenschutzaufsicht für die landeskirchlichen Stellen und die Diakonie nebst zugehörigen Einrichtungen an die Datenschutzaufsicht der EKD zu ändern. Der Kirchenausschuss könnte auch eigene Datenschutzaufsichten benennen, sowohl allein, als auch mit anderen Landeskirchen gemeinsam.

Andere Landeskirchen haben Ausführungsbestimmungen erlassen, welche nähere Ausführungen zum Datenschutzgesetz der EKD enthalten. Diese spezifizieren z. B. die Details von Vertragsvereinbarungen, wie etwa Auftragsverarbeitungsverträge.

1.5 Aus der Arbeit des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss (EDSA; engl. European Data Protection Board - EDPB) ist eine nach Art. 68 DSGVO eingerichtete, unabhängige europäische Institution, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beiträgt.

Der EDSA besteht aus den Leitern der Aufsichtsbehörden jedes Mitgliedstaates und dem Europäischen Datenschutzbeauftragten oder den jeweiligen Vertretern. Sofern wie in Deutschland mehr als eine Aufsichtsbehörde für den Datenschutz zuständig ist, ist für diesen Mitgliedstaat ein gemeinsamer Vertreter zu benennen. Diese Aufgabe wird nach den Vorgaben des BDSG durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) wahrgenommen.

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

Aufgabe des EDSAs ist nach Art. 70 Abs. 1 DSGVO die europaweit einheitliche Anwendung der Verordnung. Dafür veröffentlicht der Ausschuss nicht nur Leitlinien zur Auslegung der Kernkonzepte der DSGVO, sondern erlässt auch verbindliche Beschlüsse in Streitigkeiten über grenzüberschreitende Verarbeitungsaktivitäten und gewährleistet so eine einheitliche Anwendung von EU-Vorschriften, um zu verhindern, dass ein und dieselbe Rechtssache in verschiedenen Staaten unterschiedlich gehandhabt wird. Der EDSA spielt auch eine Rolle bei der Abgabe von Stellungnahmen zu Entscheidungsentwürfen der Aufsichtsbehörden.

Eine weitere Aufgabe des Europäischen Datenschutzausschusses besteht in der Fassung verbindlicher Beschlüsse für den Fall, dass eine betroffene Aufsichtsbehörde Widerspruch gegen den Entscheidungsentwurf der federführenden Aufsichtsbehörde einlegt, die federführende Aufsichtsbehörde den Widerspruch ablehnt (One-Stop-Shop-Verfahren) oder wenn widersprüchliche Auffassungen darüber bestehen, welche Aufsichtsbehörde federführend ist. Auch entscheidet der EDSA, wenn eine Aufsichtsbehörde nicht die (gemäß dem Kohärenzverfahren erforderliche) Stellungnahme des Ausschusses anfordert oder dieser nicht Folge leistet.

Im Jahr 2019 hat der Europäische Datenschutzausschuss Leitlinien zu den folgenden Themen veröffentlicht:

- Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679
- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR (General Data Protection Regulation, dt. DSGVO) in the context of the provision of online services to data subjects
- Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default
- Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)

Daneben hat der EDSA im Berichtszeitraum 17 Stellungnahmen verabschiedet, die sich mehrheitlich mit den von den nationalen Datenschutzaufsichten beim EDSA eingereichten Listen nach Art. 35 Abs. 4 und 5 DSGVO zur Datenschutz-Folgenabschätzung befasst haben. Daneben wurden auch folgende Stellungnahmen gefasst (Auszug):

- Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO, insbesondere in Bezug auf die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden
- Stellungnahme 8/2019 zur Zuständigkeit einer Aufsichtsbehörde im Falle einer Veränderung von Umständen, die die Hauptniederlassung oder die einzige Niederlassung betrifft

Auf der offiziellen Internetseite des EDSAs kann jeder dessen Arbeit verfolgen und aktuelle Informationen erhalten.[4]

1.6 (Neue?) Anforderungen aus der KDG-DVO für die Datensicherheit

Bei der Neuregelung des kirchlichen Datenschutzrechts hatte der Gesetzgeber die Neufassung der DVO schon vorgesehen und daher in § 57 Abs. 5 KDG eine Übergangsregelung hineingeschrieben. Danach galt die bisherige Durchführungsverordnung – soweit sie den Regelungen des neuen KDG nicht entgegenstand – bis zur Neufassung der DVO, längstens aber bis zum 30.06.2019.

Mit der Neufassung der DVO als „Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)" ist der Gesetzgeber im Frühjahr 2019 diesem Auftrag nachgekommen. Die KDG-DVO übernimmt dabei einige Regelungen der alten DVO, fügt diesen bestehenden Regelungen aber auch neue Bereiche hinzu.

Wie bereits in Abschnitt 1.3.1 erwähnt, werden in der seit März 2019 geltenden KDG-DVO praktische Konkretisierungen von Bestimmungen des KDG formuliert und somit Mindeststandards gesetzt, deren Einhaltung die Umsetzung des KDG für den Verantwortlichen erleichtern beziehungsweise konkretisieren soll.

4 Siehe https://edpb.europa.eu/edpb_de

Die konkrete Anwendbarkeit der KDG-DVO – und damit ihre Funktion als Hilfestellung für die Einrichtungen – lässt sich gut am Beispiel der Begriffe Datenschutzklasse, Schutzbedarf und Schutzniveau zeigen:

In den §§ 9 – 14 KDG-DVO wird ein dreistufiges System von Datenschutzklassen und den zugehörigen Schutzniveaus festgelegt. Jedes zu verarbeitende Datum soll nach seiner Art und dem für die Betroffenen bestehenden Risiko in eine der drei Datenschutzklassen eingeordnet werden. Die den Datenschutzklassen zugeordneten Schutzniveaus bestehen wiederum aus einer Reihe von Maßnahmen, die mit zunehmendem Schutzbedarf immer ausgeprägter sind.

Das System ist bereits aus der Vorgängerverordnung, der KDO-DVO bekannt, wird aber jetzt in der KDG-DVO konsistent hergeleitet und dargestellt. Die drei Datenschutzklassen (DSK) sind anhand des Risikos für die Betroffenen im Falle von Datenschutzverletzungen wie folgt charakterisiert:

DSK I: Die missbräuchliche Verarbeitung von Daten dieser Klasse lässt keine besonders schwerwiegende Beeinträchtigung des Betroffenen erwarten (vgl. § 11 Abs. 1 KDG-DVO).

z.B. Namens- und Adressangaben (ohne Sperrvermerke), Berufsbezeichnungen

DSK II: Die missbräuchliche Verarbeitung von Daten dieser Klasse kann den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen (vgl. § 12 Abs. 1 KDG-DVO).

z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten

DSK III: Die missbräuchliche Verarbeitung von Daten dieser Klasse kann die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen (vgl. § 13 Abs. 1 KDG-DVO).

z.B. besondere Kategorien personenbezogener Daten (§ 4 Ziff. 2 KDG), Daten über strafbare Handlungen, arbeitsrechtliche Verhältnisse, Disziplinarentscheidungen und Namens- und Adressangaben mit Sperrvermerken

Dieses System der vorgegebenen Datenschutzklassen wird von einigen Anwendern als Erschwerung der Arbeit missverstanden, da die Anwender die verarbeiteten Daten zwangsweise in eine der drei Datenschutzklassen einsortieren müssen.

Diese Interpretation der Vorgabe des Verordnungsgebers lässt außer Acht, dass der Verordnungsgeber hiermit eine typisierte Risikoeinschätzung vorgenommen hat, die den Anwendern die Arbeit erleichtert. Anders als im staatlichen Bereich hat der Verordnungsgeber sich hier für eine Konkretisierung der Einstufung entschieden.

„...eine typisierte Risikoeinschätzung ..., die den Anwendern die Arbeit erleichtert."

Ohne diese Datenschutzklassen müsste jeder Verantwortliche für eine Verarbeitung personenbezogener Daten eine individuelle Abschätzung des Risikos der konkreten Datenverarbeitung für die Rechte und Freiheiten der von der Verarbeitung betroffenen Personen vornehmen und die adäquaten Schutzmaßnahmen bestimmen.

Diese individuelle Risikoeinschätzung hat der Verordnungsgeber durch die Schaffung der drei Datenschutzklassen schon typisiert vorgenommen und den Verantwortlichen für die Datenverarbeitungen damit viel Arbeit abgenommen.

Trotz dieser typisierenden Betrachtungsweise des Risikos der Datenverarbeitung darf aber nicht vergessen werden, dass die in der KDG-DVO genannten Schutzmaßnahmen beispielhaft sind. Besondere Umstände, die über diese typisierende Betrachtung hinausgehen, erfordern möglicherweise weitergehende Schutzmaßnahmen.

Tatsächlich werden nicht nur drei Datenschutzklassen definiert, sondern genau genommen sogar fünf. Zusätzlich zu den oben genannten Klassen werden noch die Daten erwähnt, die dem Seelsorgegeheimnis unterliegen sowie die, die gemäß cc. 983 ff. CIC (Codex Iuris Canonici) sogar unter das Beichtgeheimnis fallen.

Während personenbezogene Daten, die dem Beichtgeheimnis unterliegen, nach § 14 Abs. 2 KDG-DVO gar nicht verarbeitet werden dürfen, müssen für Daten, die dem Seelsorgegeheimnis unterliegen, besondere Schutzmaßnahmen getroffen werden, die noch über die Maßnahmen der Datenschutzklasse III hinausgehen. Als Beispiele werden die Verarbeitung dieser Daten nur in eigenen Netzen ohne externe Anbindung oder die Speicherung in verschlüsselter Form genannt.

Ein weiteres Beispiel für den Willen des Verordnungsgebers, mit der KDG-DVO den Anwendern des KDG für bestimmte Verarbeitungssituationen konkrete Hinweise mit an die Hand zu geben, zeigt sich in den §§ 18 bis 26 KDG-DVO. Sie bestehen aus einer Sammlung von Vorschriften und Regelungen für spezielle Situationen, die in der täglichen Arbeit der kirchlichen Einrichtungen oft anzutreffen sind. Die wichtigsten Punkte sind dabei:

- Nur der Verantwortliche (also i.d.R. der Dienstgeber) bestimmt, welche Software auf dienstlichen Geräten installiert wird (§ 18 KDG-DVO).
- Die Nutzung dienstlicher Systeme zu privaten Zwecken ist bis auf zu begründende Einzelfälle genauso unzulässig, wie umgekehrt die dienstliche Nutzung privater Geräte (§§ 19, 20 KDG-DVO).
- Ausnahmen von den Nutzungsverboten nach den §§ 19 und 20 KDG-DVO können vom Verantwortlichen geregelt werden. Dazu ist die Schriftform nötig und im Fall einer dienstlichen Nutzung von Privatsystemen muss sich der Besitzer (also der Mitarbeitende) einem Gerätemanagement durch den Verantwortlichen unterwerfen, das nötigenfalls bis zur Löschung durch Fernzugriff reichen kann.

- Erfolgt die Wartung von IT-Systemen mit personenbezogenen Daten aus der Ferne (remote), müssen die Tätigkeiten des Dienstleisters permanent beobachtet werden. Auch sollen technische Maßnahmen getroffen werden, die ein unbefugtes Auslesen oder Kopieren der Daten verhindern (§ 21 KDG-DVO).
- Faxgeräte sollen so aufgestellt werden, dass Unbefugte keine Kenntnisse der übertragenen Nachrichten erhalten. Bei der Übertragung besonders sensibler personenbezogener Daten (Datenschutzklassen II und III) müssen zusätzliche organisatorische Maßnahmen getroffen werden, z.B. eine vorherige Absprache mit dem Empfänger über den Zeitpunkt der Übertragung, so dass dieser das Fax direkt entgegennehmen kann (§ 24 KDG-DVO).
- E-Mails mit personenbezogenen Daten der Datenschutzklassen II und III dürfen außerhalb geschlossener und gesicherter Netzwerke nur verschlüsselt übertragen werden (§ 25 KDG-DVO).

1.7 Projektgruppe „Kirchliches Datenschutzmodell (KDM)“

Zusammen mit dem Beauftragten für den Datenschutz der EKD (BfD EKD) sowie den anderen katholischen Datenschutzaufsichten in Deutschland erarbeitet das Katholische Datenschutzzentrum in einer ökumenischen Arbeitsgruppe eine kirchenspezifische Adaption des von der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder (DSK) herausgegebenen Standarddatenschutzmodells (SDM). Diese kirchenspezifische Adaption des Standarddatenschutzmodells, das Kirchliche Datenschutzmodell, soll eine Doppelfunktion wahrnehmen: es stellt ein Handwerkszeug sowohl für die Aufsichtsbehörden als auch für die verantwortlichen kirchlichen Stellen dar. Die Datenschutzaufsichtsbehörden erhalten ein Werkzeug, mit dem Vor-Ort-Prüfungen standardisiert durchgeführt werden können und kirchliche Stellen können ihre gelebte Datenschutzpraxis durch Abgleich Ihrer Maßnahmen mit dem KDM verbessern und selbst überprüfen.

Die ökumenische Arbeitsgruppe legte die konkreten Rahmenbedingungen und Vorgehensweisen für das Projekt fest. Das Kirchliche Datenschutzmodell soll die gleiche Struktur wie das Standarddatenschutzmodell aufweisen (Hauptdokument und Anlagen). Nach der Anpassung des Hauptdokumentes wird die Arbeit mit den Bausteinen erfolgen, die nach und nach im staatlichen Bereich erarbeitet werden. Es ist auch beabsichtigt, gegebenenfalls eigene Bausteine für den kirchlichen Bereich einzubinden (für Prozesse, die im außerkirchlichen Bereich nicht relevant sind).

In einem ersten Schritt wurde das Hauptdokument in kleinen ökumenischen Redaktionsteams an die kirchlichen Rechtsgrundlagen angepasst.

In der weiteren Arbeit wurde über die konkreten Überarbeitungen des Hauptdokumentes gesprochen und durch eine noch stärkere Fokussierung der Anforderungen und Bedürfnisse auf Anwender in kirchlichen Einrichtungen versucht, die Verständlichkeit für die Anwender

in kirchlichen Einrichtungen zu erhöhen. Bei allen Bearbeitungen soll durch einen intensiven Kontakt mit der DSK der direkte Bezug zum SDM nicht verloren gehen.

Für das Jahr 2020 ist die Fortsetzung der Arbeit geplant. So sollen unter anderem die Begriffe der Risikobestimmung und der Risikoanalyse anschaulich definiert und für den kirchlichen Bereich besser anwendbar gemacht werden.

Derzeit wird von der Projektgruppe als Zieltermin für eine Veröffentlichung der Ökumenische Kirchentag im Mai 2021 in Frankfurt am Main angestrebt.

2 Ausgewählte Rechtsprechung zum Datenschutzrecht

Im Berichtszeitraum wurden sowohl vom Europäischen Gerichtshof wie auch von deutschen Gerichten Entscheidungen verkündet, die wichtige Einflüsse auf die Anwendung und Auslegung der datenschutzrechtlichen Regelungen haben. Eine Auswahl dieser Entscheidungen, die auch für die Anwendung und Auslegung des kirchlichen Datenschutzrechts wichtig sind, wird nachfolgend kurz angerissen.

2.1 Europäischer Gerichtshof

Der Europäische Gerichtshof (EuGH) hat in verschiedenen Entscheidungen über datenschutzrechtliche Fragestellungen geurteilt. Insbesondere eine weitere Entscheidung zur gemeinsamen Verantwortung und eine Entscheidung zur Einwilligung sind hier hervorzuheben.

2.1.1 Urteil des EuGHs vom 29.07.2019 (Rechtssache C-40/17 – FashionID)

In diesem Vorabentscheidungsverfahren hatte der EuGH darüber zu entscheiden, welche datenschutzrechtlichen Konsequenzen die Einbindung des Facebook-Buttons haben kann.

Eine Verbraucherzentrale hatte gegen ein Unternehmen Klage erhoben, weil dieses auf seiner Internetseite den sogenannten Facebook-Button eingebunden hatte. Folge dieser Einbindung war, dass bereits durch das Aufrufen der Internetseite eine Übermittlung von Daten an Facebook erfolgt, ohne dass zuvor ein Betätigen des Facebook-Buttons erforderlich ist. In der Konsequenz bedeutet dies, dass Facebook z. B. Kenntnis davon erhält, von welcher IP-Adresse welche Internetseite aufgerufen wurde. Facebook kann dadurch Verhaltensweisen von Nutzern nachvollziehen, auch wenn diese selbst nicht Mitglied bei Facebook sind, und Informationen über die durch den Aufruf der Internetseiten gezeigten Interessen der Nutzer erlangen. Sofern die Nutzer selbst bei Facebook registriert sind, kann Facebook außerdem noch weitere Informationen gewinnen. Diese Handhabung war für den Nutzer der Internetseite nicht zwingend erkennbar. Darüber hinaus stand ihm keine Möglichkeit zur Verfügung, die Datenübermittlung zu unterbinden.

In seinem Urteil vom 29. Juli 2019 hat der EuGH zu dieser Konstellation entschieden, dass der Betreiber einer Internetseite für die Übermittlungen an Facebook als Verantwortlicher im Sinne des Datenschutzrechts anzusehen ist. Die Entscheidung bestätigt die im Urteil des EuGHs vom 5. Juni 2018 (Rechtssache C-210/16) enthaltenen Aussagen zur gemeinsamen Verantwortung von Betreibern von Facebook-Fanpages und Facebook selbst.

Nach dem Tenor der Entscheidung geht der EuGH davon aus, dass derjenige, der die Verarbeitung personenbezogener Daten der betroffenen Personen durch einen anderen Verantwortlichen veranlasst und an den Ergebnissen dieser Verarbeitung partizipiert, gemeinsam mit dem anderen für die Verarbeitung verantwortlich ist, wenn beide Parteien wechselseitig zumindest stillschweigend in die Verarbeitung des anderen einwilligen. Das gilt auch dann, wenn der Veranlassende zu keinem Zeitpunkt Kenntnis von den (durch den anderen) verarbeiteten Daten hat. Der EuGH hat den Seitenbetreiber der Internetseite und Facebook als gemeinsam Verantwortliche im Sinne des Datenschutzrechts angesehen. Selbst wenn der Seitenbetreiber nicht für eine weitere Verarbeitung der erhaltenen Daten durch Facebook verantwortlich ist, besteht eine Verantwortlichkeit für das Erheben der Daten über die Internetseite des Unternehmens und die Datenübermittlung an Facebook.

Weitergehend hat das Gericht festgestellt, dass der Betreiber einer Internetseite als (Mit-)Verantwortlicher seine Nutzer in diesen Fällen über die Datenverarbeitung informieren muss. Dazu gehört dann u.a. auch die Unterrichtung über die Datenübermittlung an Facebook und die Zwecke der Verarbeitung. Einwilligungen der Nutzer muss der Betreiber der Internetseite nach den Darlegungen des Gerichts zwar nur für die Vorgänge einholen, für die er mitverantwortlich ist, z. B. für das Erheben und die Übermittlung der Daten, jedoch hat dies zu erfolgen, bevor die Daten erhoben und übermittelt werden.

Der EuGH hat ferner herausgearbeitet, dass – sofern für die Datenverarbeitung als Begründung ein berechtigtes Interesse gemäß Art. 6 Abs. 1 lit. f) DSGVO geltend gemacht werden soll – jeder der für die Verarbeitung Verantwortlichen ein solches Interesse eigenständig verfolgen und sich bezüglich der Verarbeitung vollständig rechtfertigen muss. Im jeweiligen Einzelfall müssen die vorliegenden Interessen der Verantwortlichen und der betroffenen Nutzer gegeneinander abgewogen werden. Dabei lässt der EuGH allerdings offen, ob im Ergebnis die Erhebung und Übermittlung an Facebook mit Art. 6 Abs. 1 lit. f) DSGVO begründet werden könnte.

2.1.2 2.1.2 Urteil des EuGHs vom 01.10.2019 (Rechtssache C–673/17 - Planet 49)

In diesem Vorabentscheidungsverfahren hatte der EuGH u.a. darüber zu entscheiden, welche datenschutzrechtlichen Anforderungen an eine Einwilligung zu stellen sind.

Das Verfahren betraf u.a. die Einwilligung von Teilnehmenden an einem zu Werbezwecken veranstalteten Gewinnspiel in die Weitergabe ihrer personenbezogenen Daten an Sponsoren und Kooperationspartner des Unternehmens sowie in die Speicherung von Informationen auf ihrem Endgerät und den Zugang zu den gespeicherten Informationen. Zur Teilnahme an dem Gewinnspiel musste eine Postleitzahl eingegeben werden. In der weiteren Abfolge wurde eine Internetseite mit Eingabefeldern angezeigt. Unter diesen befanden sich zwei mit Ankreuzkästchen versehene Hinweistexte, die Aussagen zu Einwilligungen enthielten. Die Ankreuzkästchen waren bereits voreingestellt mit Häkchen versehen. Eine Teilnahme an dem Gewinnspiel war nur möglich,

wenn mindestens in dem ersten Kästchen ein Haken gesetzt war. Der Hinweistext zu diesem Kästchen enthielt u.a. eine Einverständniserklärung, dass Teilnehmende mit der Information über Angebote von Sponsoren und Kooperationspartnern des Gewinnspielveranstalters einverstanden seien.

> **„...die wirksame Einwilligung ... erfordert ein aktives Verhalten ..."**

Nach Auffassung des EuGHs erfordert die wirksame Einwilligung, dass die Einwilligung der betroffenen Person als Willensbekundung erfolgt, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden. Dies erfordert ein aktives Verhalten, welches nicht darin besteht, dass der Betreffende ein voreingestelltes Ankreuzkästchen nicht abwählt. Auch ist im Fall einer solchen Situation nicht auszuschließen, dass der Nutzer relevante Informationen nicht gelesen hat, bevor er seine Aktivitäten auf der Internetseite fortsetzt.

Ebenfalls wird die Bestätigung der Teilnahme an dem Gewinnspiel als nicht ausreichend angesehen, um von einer wirksamen Einwilligung des Betroffenen in die Speicherung von Cookies ausgehen zu dürfen. Der EuGH verweist auch auf die Regelungen der Datenschutz-Grundverordnung, wonach ausdrücklich eine aktive Einwilligung vorgesehen ist.

Weiterhin kommt der EuGH zu dem Ergebnis, dass Angaben zur Funktionsdauer von Cookies und Angaben darüber, dass Dritte Zugriff auf die Cookies erhalten können, zu den Informationen gehören, die ein Diensteanbieter den Nutzern seiner Internetseite darlegen muss.

2.2 Bundesverfassungsgericht

Auch das Bundesverfassungsgericht (BVerfG) hat im Berichtszeitraum für den Datenschutz wichtige Urteile gefällt. An dieser Stelle sollen die beiden Entscheidungen „Recht auf Vergessen" I und II kurz angerissen werden.

2.2.1 Beschluss des BVerfGs vom 6.11.2019 (1 BvR 16/13 - Recht auf Vergessen I)

Dem Beschluss des Bundesverfassungsgerichts liegt ein Sachverhalt über die Bereithaltung von mehr als 30 Jahre zurückliegenden Presseberichten in einem Online-Archiv zugrunde. In diesen Presseberichten wurde unter namentlicher Nennung über die strafrechtliche Verurteilung des Beschwerdeführers wegen Mordes berichtet. Der Bericht eines Magazins war in dem Archiv kostenlos abrufbar und wurde auch bei namentlicher Eingabe des Beschwerdeführers in einem Internetportal unter den ersten Treffern angezeigt.

Der Bundesgerichtshof hatte den Unterlassungsanspruch des Klägers verneint und im Rahmen einer Abwägung die Interessen des Beschwerdeführers geringer bewertet als das Informationsinteresse der Öffentlichkeit und das Recht auf freie Meinungsäußerung der Presse.

Das BVerfG hat die Verfassungsbeschwerde des Beschwerdeführers für zulässig und begründet gehalten. Der Erste Senat kommt zu dem Ergebnis, dass der Beschwerdeführer in seinem allgemeinen Persönlichkeitsrecht verletzt ist.

Das BVerfG äußert sich in seinem Beschluss daneben ausführlich zu Fragestellungen der Grundrechte des Grundgesetzes (GG) als Beurteilungsmaßstab sowie zur Berücksichtigung von Anwendungsbereichen des Unionsrechts, wie etwa der Charta der Grundrechte der Europäischen Union (GRCh).

In der Entscheidung führt der Erste Senat an, dass die Rechtsordnung auch davor schützen muss, dass sich eine Person frühere Positionen, Äußerungen und Handlungen unbegrenzt vor der Öffentlichkeit vorhalten lassen muss. Der Senat stellt darauf ab, dass erst die Ermöglichung eines Zurücktretens zurückliegender Sachverhalte dem Einzelnen die Chance zum Neubeginn in Freiheit gibt, wobei zur Zeitlichkeit der Freiheit auch die Möglichkeit des Vergessens gehört. Allerdings weist der Senat darauf hin, dass aus dem allgemeinen Persönlichkeitsrecht kein Anspruch folgt, alle personenbezogenen Informationen, die im Rahmen von Kommunikationsprozessen ausgetauscht wurden, aus dem Internet entfernen zu lassen. Den Betroffenen steht auch kein Recht zu, nach ihren eigenen Vorstellungen die öffentlich zugänglichen Informationen filtern zu dürfen und insoweit Beschränkungen der Darstellungen über die eigene Person vornehmen zu können.

Im Rahmen der Prüfung ist ein Grundrechtsausgleich zu thematisieren. Zugunsten des Beschwerdeführers wertet das BVerfG das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Zu diesem gehört nach den Ausführungen des Gerichts als eigenständige Ausprägung auch das Recht auf informationelle Selbstbestimmung. Demgegenüber sind Meinungsfreiheit und Pressefreiheit als Grundrechte abzuwägen. In der konkreten Ausprägung gewährt das allgemeine Persönlichkeitsrecht einen Schutz vor Verbreitung von Berichten, die das Ansehen eines Betroffenen in einer seine Persönlichkeitsentfaltung gefährdenden Weise herabsetzen können. Das Gericht sieht dies auch bei Presseberichten über Straftaten als möglich an. Demgegenüber gehört es allerdings zu den Aufgaben der Presse, über Straftaten und Täter zu berichten. Darüber hinaus ist nach Auffassung des Gerichts ebenfalls zu berücksichtigen, welche Möglichkeiten zum Abruf von Informationen durch die Recherchen im Internet möglich sind und wie sich dies auf die Beeinträchtigungen des Betroffenen auswirken kann. Durch die Möglichkeit einer dauerhaften Verfügbarkeit von Informationen wird nach Auffassung des Senats die Bedeutung einer personenbezogenen Berichterstattung für den Betroffenen erheblich verändert. Aus Sicht des Senats gehört die Möglichkeit des Vergessens zur Zeitlichkeit der Freiheit. Dies wiederum darf nach Ansicht des Senats nicht dazu führen, dass allein der Betroffene über die Entscheidungshoheit verfügt, welche Daten noch zugänglich sein

dürfen und welche Informationen über ihn zu löschen sind. So weit reicht nach Einschätzung des Gerichts das Recht auf Vergessenwerden nicht. Im Rahmen der konkreten Bewertung ist auch das Verstreichen von Zeit zu berücksichtigen und die sich möglicherweise ändernde Bedeutung von Informationen.

2.2.2 Beschluss des BVerfGs vom 6.11.2019 (1 BvR 276/17 - Recht auf Vergessen II)

Das Bundesverfassungsgericht hatte in dem Verfahren über eine Verfassungsbeschwerde zu urteilen, die mit Beschluss des Gerichts zurückgewiesen wurde.

Diese Verfassungsbeschwerde betraf das Verfahren einer Beschwerdeführerin gegen einen Suchmaschinenbetreiber. Bei Eingabe des vollständigen Namens der Beschwerdeführerin wurde im Suchergebnis der Suchmaschine unter anderem ein Link zu einem mehr als sechs Jahre zurückliegenden Beitrag eines Fernsehsenders angezeigt. Dagegen machte die Beschwerdeführerin einen Anspruch auf Unterlassung dieser Anzeige geltend.

In einem Fernsehbeitrag über die Kündigungspraxis von Arbeitgebern hatte ein Fernsehsender auch über einen die Beschwerdeführerin als Arbeitgeberin betreffenden Fall berichtet. Bei Eingabe des vollständigen Namens der Beschwerdeführerin in die Maske der Internetsuchmaschine wurde als eines der ersten Ergebnisse die Verlinkung auf den Fernsehbeitrag angezeigt. Dies erfolgte auch noch längere Zeit nach Ausstrahlung des Beitrags. Die Beschwerdeführerin hatte zunächst in gerichtlichen Verfahren die Entfernung des Links zum Transskript des Fernsehbeitrags oder die Unterlassung der Weiterleitung auf diesen Link geltend gemacht. Das mit dem Verfahren zuletzt befasste Oberlandesgericht Celle hatte die Klage der Beschwerdeführerin abgewiesen und die Speicherung des streitgegenständlichen Links für zulässig gehalten. Einen Anspruch der Beschwerdeführerin auf Auslistung bei der Suchmaschine hat das Gericht verneint. Begründet wurde dies unter anderem damit, dass die Daten aus allgemein zugänglichen Quellen, wie dem öffentlich zugänglichen Archiv des Rundfunksenders, stammten und nach Auffassung des Oberlandesgerichts die schutzwürdigen Interessen der Beschwerdeführerin am Ausschluss der Speicherung nicht offensichtlich überwiegend seien.

Mit der Verfassungsbeschwerde rügt sie nunmehr eine Verletzung ihres allgemeinen Persönlichkeitsrechts und ihres Grundrechts auf informationelle Selbstbestimmung.

Die zulässige Verfassungsbeschwerde ist nach Auffassung des Bundesverfassungsgerichts unbegründet. In der Entscheidung hat der Erste Senat zugebilligt, dass sich die Beschwerdeführerin auch auf die Grundrechte der Charta der Grundrechte der Europäischen Union berufen kann. Zugunsten der Beschwerdeführerin stellt der Senat auf die Achtung des Privat- und Familienlebens aus Art. 7 GRCh und auf den Schutz personenbezogener Daten aus Art. 8 GRCh ab. Dem gegenüber stellt das BVerfG für die Bewertung der Interessen des beklagten

Suchmaschinenbetreibers dessen Recht auf unternehmerische Freiheit aus Art. 16 GRCh mit der Gewährleistung der Verfolgung wirtschaftlicher Interessen durch das Angebot von Waren und Dienstleistungen.

Der Senat stellt im Rahmen seiner Entscheidung ebenfalls heraus, dass es bei der Beurteilung der Wirkung von namensbezogenen Suchabfragen für die Gewichtung der Grundrechtseinschränkung maßgeblich auf die Wirkung der Verbreitung der Informationen ankommt. In diesem Zusammenhang ist auch die Frage der Zugänglichkeit der Informationen durch Suchmaschinen zu berücksichtigen. Im Ergebnis ist nach Auffassung des Ersten Senats die angegriffene Entscheidung des Oberlandesgerichts nicht zu beanstanden. Zwar hat das Oberlandesgericht nicht verkannt, dass durch Zeitablauf die identifizierende Verbreitung von Medienbeiträgen durch Suchmaschinen unzumutbar und damit unzulässig werden kann. Im konkreten Fall ist dieser Zeitpunkt aber als noch nicht erreicht angesehen worden. Diese Auffassung teilt der Erste Senat. Zu Lasten der Beschwerdeführerin ist gewertet worden, dass sie mit einem Interview selbst in die Öffentlichkeit getreten ist und dass an dem Thema ein nach wie vor fortdauerndes öffentliches Interesse besteht. Auch ist der Zeitraum von sieben Jahren bezüglich der fortdauernden Aktualität des Themas als nicht zu lang angesehen worden.

2.3 Bundesverwaltungsgericht

Aus der Rechtsprechung des Bundesverwaltungsgerichts (BVerwG) im Berichtszeitraum werden nachfolgend zwei Entscheidungen zur Videoüberwachung und zu Facebook-Fanpages vorgestellt.

2.3.1 Urteil des BVerwGs vom 27.03.2019 (6 C 2.18 - Videoüberwachung)

Die Entscheidung des Bundesverwaltungsgerichts betrifft den Bereich der Videoüberwachung, konkret die in einer Zahnarztpraxis. Zur Überwachung des Empfangsbereichs befand sich eine Digitalkamera oberhalb des Tresens der Praxis, die Bilder in Echtzeit lieferte. Diese Bilder konnten auf Monitoren eingesehen werden, die von der Zahnärztin in den Behandlungszimmern aufgestellt waren. Überwacht wurden Bereiche hinter dem Empfangstresen sowie die, in denen sich Besucher nach einem ungehinderten Betreten der Praxis aufhalten konnten. Auf der Außenseite der Eingangstür und am Tresen war die Aufschrift „videogesichert“ angebracht.

Der zuständige Landesdatenschutzbeauftragte hatte der Zahnärztin aufgegeben, dass die Kamera so auszurichten sei, dass die Bereiche, die den Besuchern offenstehen, während der Öffnungszeiten der Praxis nicht mehr erfasst werden.

Das bisherige Klageverfahren hatte mit einer Entscheidung des Oberverwaltungsgerichts (OVG) geendet. Dieses hatte den Einsatz des

Kamera-Monitor-Systems als unzulässige Videoüberwachung angesehen. Eine solche Maßnahme solle Privatpersonen nur dann gestattet sein, wenn die Betroffenen zustimmten oder die gesetzlichen Zulässigkeitsvoraussetzungen vorlägen. Das Vorliegen dieser Voraussetzungen hatte das OVG verneint. Auch die angebrachten Hinweisschilder führten nach Auffassung des Gerichts nicht dazu, dass die Besucher der Praxis mit der Beobachtung einverstanden seien und sie etwa durch ihr Betreten dieses Einverständnis erklärten. Ferner ging das Gericht davon aus, dass keine Anhaltspunkte vorlägen, die ein erhöhtes Risiko für die Begehung von Straftaten gegen die Zahnärztin erkennen ließen. Als geeignete Maßnahme könnte an Stelle der Videoüberwachung auch die Besetzung des Empfangstresens mit einem Mitarbeitenden in Betracht kommen. Bei einer Abwägung überwiegen die Interessen der Besucher die entgegenstehenden Interessen der Klägerin.

Das BVerwG hat die zulässige Revision der Zahnärztin als nicht begründet angesehen. Ein Verstoß gegen Bundesrecht wurde nicht angenommen. Vielmehr wurde bestätigt, dass das OVG zutreffend angenommen habe, dass die Beobachtung unzulässig sei. Sie sei auch nicht erforderlich, um berechtigte Interessen der Zahnärztin zu wahren. Der Landesdatenschutzbeauftragte konnte daher auch eine andere Ausrichtung der Kamera aufgeben. Die Anordnung des Landesdatenschutzbeauftragten wurde als ermessensfehlerfrei und verhältnismäßig beurteilt.

Das BVerwG hat das Vorliegen einer Datenverarbeitungsanlage im Sinne von § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes alter Fassung (BDSG a. F.), welches der Entscheidung zugrunde zu legen war, bejaht. Weiterhin wurde in der vorgenommenen Installation ein Verstoß gegen die Vorschriften des Datenschutzes im Sinne von § 38 Abs. 5 S. 1 BDSG a. F. gesehen, weil die Betroffenen nicht eingewilligt hatten und die Zulässigkeitsvoraussetzungen des § 6 b Abs. 1 BDSG a. F. nach Auffassung des Gerichts nicht vorlagen.

Bezüglich der rechtswirksamen Einwilligung hat das Gericht darauf abgestellt, dass diese auf einer freien Entscheidung beruhen muss. Die Betroffenen müssen auf den vorgesehenen Zweck der Maßnahme hingewiesen werden und die Einwilligung bedarf der Schriftform nach früherem Recht, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die angebrachten Hinweise auf die Beobachtung führen dabei nicht zu dem Ergebnis, dass die Patienten rechtswirksam einwilligen, wenn sie unter Kenntnis dieses Hinweisschildes die Praxis weiter betreten.

Eine mögliche Rechtfertigung der Videoüberwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke hat das Gericht vorliegend nicht bejaht.

Weiterhin hat das Gericht dem Landesdatenschutzbeauftragten eine rechtsfehlerfreie Ermessensausübung bestätigt.

Ferner wurde ausgeführt, dass die Rechtsänderung mit der Datenschutz-Grundverordnung und deren Inkrafttreten am 25. Mai 2018 keine Auswirkungen auf die Beurteilung der Rechtmäßigkeit der Anordnung und auf die Revisionsentscheidung hat.

2.3.2 Urteil des BVerwGs vom 11.09.2019 (6 C 15.18 - Facebook-Fanpages)

Die Entscheidung des Bundesverwaltungsgerichts befasst sich mit einem Verfahren, in dem einer gemeinnützigen Bildungseinrichtung durch die zuständige Datenschutzaufsicht auferlegt worden war, die von der Bildungseinrichtung unterhaltene Facebook-Seite, die sogenannte Facebook-Fanpage, zu deaktivieren.

Die Bildungseinrichtung betreibt im sozialen Netzwerk von Facebook einen Benutzer-Account in Form einer Fanpage, auf dem sie sich und ihre Angebote präsentiert.

Die Datenschutzaufsicht hatte die Deaktivierung dieser Fanpage vor dem Hintergrund angeordnet, dass Facebook bei Aufruf dieser Fanpage Cookies setzen würde, die zu einer Verarbeitung personenbezogener Daten der Nutzer und zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung führten. Über die Art, den Umfang und die Zwecke der Datenerhebung sowie über das Bestehen eines Widerspruchsrechts gegen die Erstellung eines Nutzungsprofils hat die Bildungseinrichtung ihre Nutzer nicht unterrichtet. Darüber hinaus hat sie auch keine Möglichkeit vorgesehen, ein Widerspruchsrecht auszuüben.

Facebook erstellt aus den Nutzerdaten zumindest anonymisierte statistische Zusammenstellungen, die über die Funktion „Facebook Insights“ vom Fanpagebetreiber, hier also der Bildungseinrichtung, zur Analyse des Nutzungsverhaltens abgerufen werden können.

Die Datenschutzaufsicht hat die Bildungseinrichtung datenschutzrechtlich für die Verarbeitung der Nutzerdaten auch bezüglich der von Facebook vorgenommenen Datenverarbeitungsvorgänge für verantwortlich gehalten. Diese Verantwortlichkeit beruht darauf, dass die Bildungseinrichtung durch den Betrieb der Fanpage Facebook erst den Zugriff auf die Daten der Nutzer eröffnet und sie im Gegenzug von den Vorteilen der durch Facebook unentgeltlich zur Verfügung gestellten Infrastruktur und der möglichen Informationsgewinnung profitieren möchte.

Zwischenzeitlich mit Facebook geführte Gespräche hatten keine aus Sicht der Datenschutzaufsicht zufriedenstellende Lösung erbracht. Daher kam die Datenschutzaufsicht zu dem Ergebnis, dass allein die Deaktivierung der Fanpage einen datenschutzkonformen Zustand herstellen kann.

Das Argument der Bildungseinrichtung richtete sich darauf, dass sie lediglich Nutzerin des sozialen Netzwerks und an die vorgegebene Infrastruktur gebunden sei. Für von Facebook vorgenommene Datenverarbeitungen trage sie selbst keine Verantwortung. Weiterhin führte sie an, dass die Facebook-Nutzer im Rahmen ihrer Registrierung und wegen der Annahme der Facebook-Nutzungsbedingungen in die Datenverarbeitungen eingewilligt hätten. Auch Nutzer, die selbst nicht bei Facebook registriert seien, könnten sich über die Nutzungsbedingungen informieren.

Auf Seiten der Bildungseinrichtung und von Facebook wurde weiter damit argumentiert, dass ein Facebook-Fanpagebetreiber die Datenerhebungen von Facebook und auch die Verarbeitung im Rahmen der Facebook Insights-Funktion nicht beeinflussen könne. Daher könne ein Betreiber einer Facebook-Fanpage auch nicht verantwortliche Stelle sein.

Das zunächst angerufene Verwaltungsgericht hat den angefochtenen Bescheid in Gestalt des Widerspruchsbescheides aufgehoben und die Bildungseinrichtung nicht als verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes alter Fassung angesehen. Auch das Oberverwaltungsgericht in der nächsten Instanz war davon ausgegangen, dass mangels Kontroll- und Einflussmöglichkeiten keine datenschutzrechtliche (Mit-)Verantwortlichkeit der Bildungseinrichtung für die Datenverarbeitungsvorgänge in Bezug auf Facebook begründet werden könnte. Dagegen hatte die Datenschutzaufsicht Revision eingelegt.

Der Erste Senat des BVerwGs hatte im Revisionsverfahren mit Beschluss vom 25. Februar 2016 das Verfahren ausgesetzt und in einem sogenannten Vorabentscheidungsverfahren den Europäischen Gerichtshof um Auslegung mehrerer Bestimmungen der Datenschutzrichtlinie (die als europäische Richtlinie dem BDSG zugrunde liegt) gebeten. Mit Urteil vom 5. Juni 2018 unter dem Aktenzeichen C-210/16 hat der EuGH festgestellt, dass der Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage für die Verarbeitung ein Verantwortlicher im Sinne des Art. 2 Buchst. d der Datenschutzrichtlinie ist. Bestätigt wurde auch, dass das deutsche Datenschutzrecht anwendbar ist, da die amerikanische Muttergesellschaft Facebook Inc. mit der Facebook Germany GmbH in Deutschland über eine dauerhafte Niederlassung verfügt und die beanstandeten Verarbeitungen in den Rahmen der Tätigkeit dieser Niederlassung fallen.

Das BVerwG hat die Revision als begründet angesehen, soweit dadurch Rechtsverletzungen bestehen. Sie hat das Berufungsurteil aufgehoben und die Sache an das OVG zurückgewiesen, da die bisherigen Feststellungen des Berufungsgerichts als nicht ausreichend angesehen wurden, um die Rechtmäßigkeit der Datenverarbeitungsvorgänge zu beurteilen. Auch hat das BVerwG den Maßstab, mit dem das Berufungsgericht die datenschutzrechtliche Verantwortlichkeit beurteilt hat, vor dem Hintergrund der Vorgaben des EuGHs als mit dem Bundesrecht unvereinbar angesehen.

Die Auslegung des Begriffs der verantwortlichen Stelle wurde aus Sicht des BVerwGs durch das OVG nicht zutreffend vorgenommen. Unter Berücksichtigung der Entscheidung des EuGHs ist nach den Vorstellungen des BVerwGs der Begriff des Verantwortlichen unionsrechtskonform dahingehend zu verstehen, dass er auch Stellen erfasst, die anderen die Gelegenheit der Datenverarbeitung einräumen, ohne selbst damit befasst zu sein. Der EuGH hatte festgestellt, dass der Begriff des für die Verarbeitung Verantwortlichen in der der Entscheidung zugrunde liegenden Regelung des Art. 2 Buchst. d der Datenschutzrichtlinie den Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage mitumfasst. Dabei werden jede natürliche oder juristische Person und jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entschei-

det, als für die Verarbeitung verantwortliche Stelle angesehen. Der Betreiber einer auf Facebook unterhaltenen Fanpage gibt die Möglichkeit, auf dem Computer oder einem anderen Gerät des Nutzers, der die Fanpage besucht, Cookies zu platzieren, unabhängig davon, ob diese Person selbst über ein Facebook-Konto verfügt. Dadurch hat nach Auffassung des EuGHs der Betreiber einen maßgeblichen Beitrag zur Verarbeitung personenbezogener Daten der Besucher der Fanpage gesetzt. Für die Bejahung einer datenschutzrechtlichen Verantwortlichkeit ist nach Auffassung des EuGHs nicht erforderlich, dass bei einer gemeinsamen Verantwortlichkeit mehrerer Betreiber für dieselbe Verarbeitung jeder den Zugang zu den betreffenden personenbezogenen Daten hat. Daher ist der Betreiber einer Fanpage an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher der Fanpage beteiligt und damit auch für die Verarbeitung Verantwortlicher. Er muss demzufolge auch die Verpflichtungen, die im Bereich des Schutzes personenbezogener Daten auftreten, erfüllen.

Das Bundesverwaltungsgericht hat der zuständigen Datenschutzaufsicht außerdem bestätigt, dass sie das anzuwendende Ermessen rechtmäßig ausgeübt hat.

Bestätigt wurde weiterhin, dass auch im Bereich des Datenschutzes unter dem Gebot einer effektiven und wirkungsvollen Gefahrenabwehr es gerechtfertigt sein kann, denjenigen Verantwortlichen heranzuziehen, dessen Pflichtigkeit sich ohne weiteres bejahen lässt und dem effektive Mittel zum Abstellen des Verstoßes zur Verfügung stehen. Daher durfte nach Auffassung des Gerichts die Datenschutzaufsicht die Anordnung der Deaktivierung gegenüber der Bildungseinrichtung vornehmen und musste nicht gegen Facebook vorgehen. Die Deaktivierungsanordnung wurde durch das Gericht als effektives und zulässiges Mittel zum Schutz der personenbezogenen Daten angesehen.

2.4 Bundesarbeitsgericht - Urteil des BAGs vom 28.03.2019 (8 AZR 421/17)

Das Bundesarbeitsgericht (BAG) hatte im Revisionsverfahren über eine Schadensersatzklage im Zusammenhang mit einer Kündigung zu entscheiden. Dabei spielte die vom Arbeitgeber eingesetzte Videoüberwachung eine Rolle. Der Arbeitgeber hatte in seinem Ladenlokal mehrere Kameras installiert, die unterschiedliche Bereiche der Räumlichkeiten abdeckten und Aufzeichnungen fertigten. Die Aufnahmen wurden mittels eines Festplattenvideorecorders aufgezeichnet, der sich in einem verschlossenen Metallbehälter befand.

Das in der Vorinstanz befasste Landesarbeitsgericht (LAG) hatte bezüglich der Videoaufzeichnungen entschieden, dass für die Einbringung der Videosequenzen in das Verfahren sowie einer möglichen Vernehmung einer Mitarbeiterin, welche die Videoaufzeichnungen ausgewertet hatte, ein Beweisverwertungsverbot aus Gründen des Daten- und Persönlichkeitsrechtsschutzes bestehen würde.

Das BAG entschied bezüglich der Revision, dass mit der auf ein Beweisverwertungsverbot gestützten Begründung keine Klageabweisung hätte erfolgen dürfen. Nach Auffassung des Senats hätte eine umfassendere Prüfung in der Vorinstanz erfolgen müssen, ob die Verwertung der nach Auffassung des LAGs datenschutzrechtlich unzulässig gewonnenen Erkenntnisse oder der Beweismittel durch das Gericht im Einzelfall einen Grundrechtsverstoß darstellen würde. Das BAG hat ausgeführt, dass es auf die Frage ankomme, ob ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliege und ob dieser Eingriff zulässig sei. Sofern ein Beweisverwertungsverbot nicht in Betracht komme, weil eine Datenerhebung und -verwertung nach den Bestimmungen des im Fall entscheidungserheblichen BDSG alter Fassung erfolgen durfte, müsse durch das entscheidende Gericht weiter geprüft werden, ob die Verwertung der so gewonnenen Beweismittel durch dieses Gericht im Einzelfall einen Grundrechtsverstoß darstelle. Dabei verweist das BAG darauf, dass Zivilprozessordnung und Arbeitsgerichtsgesetz keine Bestimmungen enthalten, welche die Verwertbarkeit von Erkenntnissen oder Beweismitteln einschränken, die eine Arbeitsvertragspartei rechtswidrig erlangt hat. Ein Verwertungsverbot kann sich nach Auffassung des Senats allerdings aus einer verfassungskonformen Auslegung des Verfahrensrechts ergeben. Ein verfassungsrechtliches Verwertungsverbot kommt dabei in Betracht, wenn dies wegen einer grundrechtlich geschützten Position einer Prozesspartei zwingend geboten ist. Voraussetzung dafür ist nach Auffassung des Gerichts in aller Regel, dass bereits durch die Informations- oder Beweisbeschaffung das allgemeine Persönlichkeitsrecht einer Partei verletzt worden ist, ohne dass dies durch überwiegende Belange der anderen Partei gerechtfertigt wäre. Ferner muss die prozessuale Verwertung der Beweismittel selbst einen Grundrechtsverstoß darstellen.

Ein Verwertungsverbot kommt bereits dann nicht in Betracht, wenn eine Maßnahme nach datenschutzrechtlichen Vorschriften, wie im entscheidungserheblichen Fall der Anwendung des BDSG alter Fassung, zulässig ist. Erst wenn die datenschutzrechtlichen Bestimmungen keine Erlaubnis vorsehen, muss weiter geprüft werden, ob die Verwertung der Erkenntnisse oder Beweismittel durch das Gericht einen Grundrechtsverstoß darstellen würde. Liegt im Ergebnis ein Beweisverwertungsverbot vor, so bezieht sich dieses auch auf mittelbare Verwertungen von Erkenntnissen, etwa auf die Vernehmung von Zeugen über den Inhalt eines Beweismittels. Das BAG hat darüber hinaus noch weitere Überlegungen angestellt, in welchen Fällen eine Unverhältnismäßigkeit der Datenerhebung durch die Videoüberwachung vorliegen kann. Der erkennende Senat des BAGs hat dazu zwar allgemein ausgeführt, sich aber wegen der bisher getroffenen Feststellungen des LAGs nicht in der Lage gesehen, konkret zu entscheiden.

2.5 Die Datenschutzgerichte der katholischen Kirche

Parallel zur Anpassung des kirchlichen Datenschutzrechts an die Europäische Datenschutz-Grundverordnung im Jahr 2018 hat die Deutsche Bischofskonferenz eigene kirchliche Gerichte errichtet, die den Rechtsschutz für Streitigkeiten aus der Anwendung des neuen kirchlichen Datenschutzgesetzes sicherstellen.

2.5.1 Die Gerichte

Für die Gewährleistung eines der Europäischen Datenschutz-Grundverordnung vergleichbaren Datenschutzes wird von den Kirchen die Sicherstellung bestimmter Vorgaben in ihren Gesetzen durch Art. 91 DSGVO verlangt. Neben der Anpassung der datenschutzrechtlichen Regelungen an die DSGVO gehört dazu die Einrichtung durchsetzungsfähiger Datenschutzaufsichten. Darüber hinaus sieht die DSGVO in ihren Regelungen die Möglichkeit des gerichtlichen Rechtsbehelfs vor. Eine solche konkret auf den Datenschutz bezogene Rechtsbehelfsmöglichkeit kannte das kirchliche Recht bisher nicht. Für die Realisierung eines der DSGVO gleichwertigen Datenschutzes bestand Einigkeit, dass eine geeignete gerichtliche Möglichkeit geschaffen werden sollte. Der kirchliche Gesetzgeber hat daher in § 49 KDG ausdrücklich geregelt, dass das Recht auf einen gerichtlichen Rechtsbehelf besteht.

Zur Umsetzung dieser Anforderung sind kirchliche Gerichte in Datenschutzangelegenheiten geschaffen und eine Kirchliche Datenschutzgerichtsordnung (KDSGO) in Kraft gesetzt worden. Für den Erlass der KDSGO als Gesetz der Deutschen Bischofskonferenz - und nicht als Gesetz jedes einzelnen Diözesanbischofs - wurde ein besonderes Mandat des Apostolischen Stuhles eingeholt.

Die Bischöfe der (Erz-)Bistümer im Bereich der Deutschen Bischofskonferenz haben als kirchliche Gerichte in Datenschutzangelegenheiten ein Interdiözesanes Datenschutzgericht (IDSG) als erste Instanz und als zweite Instanz ein Datenschutzgericht der Deutschen Bischofskonferenz errichtet. Die Kosten für diese Gerichte trägt der Verband der Diözesen Deutschlands.

Die grundsätzliche Zuständigkeit dieser Gerichte erstreckt sich auf die Überprüfung von Entscheidungen der Datenschutzaufsichten der katholischen Kirche sowie auf gerichtliche Rechtsbehelfe Betroffener gegen Verantwortliche oder kirchliche Auftragsverarbeiter. Gemäß ausdrücklicher Festlegung im Gesetz findet eine Überprüfung der Rechtmäßigkeit von kirchlichen Rechtsnormen in Form eines Normenkontrollverfahrens nicht statt.

Die Richter der kirchlichen Gerichte in Datenschutzangelegenheiten sind an das staatliche und kirchliche Recht gebunden. Ausdrücklich festgelegt ist, dass sie ihr Amt unparteiisch und in richterlicher Unabhängigkeit ausüben. Mit dieser Vorgabe ist sichergestellt, dass die erforderliche richterliche Unabhängigkeit ausdrücklich gewahrt ist und keinerlei Beeinflussung erfolgen darf. Zur Sicherstellung der fachlichen

Qualifikation müssen die Vorsitzenden und ihre Stellvertreter die Befähigung zum Richteramt nach dem Deutschen Richtergesetz sowie die weiteren Richter entweder diese Befähigung oder aber einen akademischen Grad im kanonischen Recht besitzen. Mit diesen Besetzungsvorgaben zeigt die katholische Kirche, dass sie das Erfordernis der Vergleichbarkeit mit den Vorgaben der DSGVO auch für den gerichtlichen Rechtsbehelf umsetzt. Das erteilte Mandat des Apostolischen Stuhles zeigt, dass diese Besetzung von der maßgebenden kirchlichen Autorität akzeptiert ist.

Für das Interdiözesane Datenschutzgericht ist der Amtsermittlungsgrundsatz vorgegeben. Das Datenschutzgericht der Deutschen Bischofskonferenz legt den Tatbestand, der in der ersten Instanz ermittelt wurde, zugrunde, kann aber auch im Bedarfsfall eigenständig Beweise erheben.

Auf der Seite der Deutschen Bischofskonferenz werden die Entscheidungen des Interdiözesanen Datenschutzgerichts veröffentlicht[5].

2.5.2 Die Rechtsprechung des Interdiözesanen Datenschutzgerichts

Das Interdiözesane Datenschutzgericht hat im Berichtszeitraum zwei Entscheidungen veröffentlicht, die unter den Aktenzeichen IDSG 01/2018 und IDSG 03/2018 geführt werden.

Ausgangspunkt der Entscheidung IDSG 01/2018 waren Informationsweitergaben über ein Kind des Antragstellers durch Mitarbeiterinnen der Kindertageseinrichtung, welche dieses Kind besuchte. Eine Informationsweitergabe an den Allgemeinen Sozialdienst des örtlichen Landratsamtes war zunächst in anonymisierter Form erfolgt, welche durch eine telefonische Information über Namen und Anschrift der Familie des Antragstellers ergänzt wurde. Dies führte dann zu einem unangemeldeten Hausbesuch bei der Familie des Antragstellers.

Der Antragsteller hatte von der zuständigen Datenschutzaufsicht eine Feststellung von Datenschutzverletzungen in diesem Zusammenhang begehrt. Dies wurde jedoch ablehnend beschieden. Begründet wurde die Ablehnung mit dem Vorliegen rechtfertigender Rechtsgrundlagen aus dem Sozialgesetzbuch VIII für die Datenübermittlungen seitens der Kindertagesstätte.

Der Antragsteller hatte die Feststellung begehrt, dass der Bescheid der Datenschutzaufsicht rechtswidrig sei, und weiterhin dessen Aufhebung sowie die Feststellung, dass die Weitergabe seiner Sozialdaten durch Mitarbeiterinnen der Kindertagesstätte gegen kirchliches Datenschutzrecht verstoßen habe.

Das Interdiözesane Datenschutzgericht hat die gestellten Anträge für zulässig, aber unbegründet gehalten. Es hat keinen Verstoß gegen kirchliches Datenschutzrecht in der Weitergabe der Sozialdaten des

5 Siehe www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen/

Antragstellers gesehen und das Vorliegen von Rechtfertigungsgründen aufgrund sozialrechtlicher Vorschriften bejaht. Weiterhin wurde die Vorgehensweise der Mitarbeiterinnen der Kindertagesstätte auch als verhältnismäßig eingestuft. Die Zuständigkeit der Datenschutzaufsicht für den Erlass des Bescheides wurde in der Sache bejaht und die Entscheidung als rechtmäßig bewertet.

In der Entscheidung IDSG 03/2018 wurden die Anträge des Antragstellers als unbegründet zurückgewiesen. Die Entscheidung ist jedoch noch nicht rechtskräftig, da Rechtsmittel zum Datenschutzgericht der Deutschen Bischofskonferenz als zweite Instanz eingelegt wurde.

Das Gericht hatte einen Fall zu beurteilen, bei dem eine eventuelle Datenschutzverletzung durch Informationsweitergaben im Zusammenhang mit einem möglichen Missbrauchsfall vorgetragen wurde.

Der Antragsteller hatte beantragt, sowohl die örtlich zuständige Datenschutzaufsicht, als auch die örtliche Diözese zu verpflichten, in seinem Anliegen Bescheide zu erteilen. Weiterhin begehrte er die Feststellung, dass die Weitergabe seines Falls an eine Staatsanwaltschaft und die Informierung einer weiteren Person gegen kirchliches Datenschutzrecht verstoßen würde.

Das IDSG hat die gestellten Anträge vor dem Hintergrund der dargelegten Sachverhalte ausgelegt und für zulässig, aber unbegründet erachtet.

Nach Auffassung des Interdiözesanen Datenschutzgerichts steht dem Antragsteller kein Anspruch auf Erteilung von Bescheiden in dem von ihm gewünschten Sinne zu. Das Vorliegen eines Datenschutzverstoßes, der Gegenstand eines solchen Bescheides sein könnte, hat das Gericht verneint. Darüber hinaus hat das Gericht festgestellt, dass die gerügten Weitergaben von Daten nicht gegen kirchliches Datenschutzrecht verstoßen haben, da für die Weitergaben einschlägige Rechtsgrundlagen vorliegen. Ferner waren einige Informationen beim Empfänger bereits bekannt.

Aufgrund des eingelegten Rechtsmittels ist abzuwarten, wie das Datenschutzgericht der Deutschen Bischofskonferenz entscheiden wird.

3 Aus der Tätigkeit des Datenschutzzentrums

3.1 Die betrieblichen Datenschutzbeauftragten

Die Funktion des betrieblichen Datenschutzbeauftragten ist nicht neu. Auch in der bis Mai 2018 geltenden Anordnung über den kirchlichen Datenschutz gab es schon die Verpflichtung zur Bestellung von betrieblichen Datenschutzbeauftragten. Mit der Einführung des KDG im Mai 2018 sind die betrieblichen Datenschutzbeauftragten endgültig eine feste Größe in den kirchlichen Einrichtungen und Organisationseinheiten geworden. Die immer komplexeren Verarbeitungen personenbezogener Daten und die gestiegene Sensibilität der Betroffenen im Umgang mit ihren persönlichen Daten machen die betrieblichen Datenschutzbeauftragten zu einer wichtigen fachkundigen Ansprechperson für die Verantwortlichen in den kirchlichen Einrichtungen.

Aus den Anfragen und Rückmeldungen der kirchlichen Stellen kann entnommen werden, dass die betrieblichen Datenschutzbeauftragten stärker als früher in die betrieblichen Prozesse und Entscheidungen einbezogen werden, um die kirchlichen Stellen in Fragen des Datenschutzes zu beraten. Dies ist ein positiver Trend, aber noch kein Grund für die Einrichtungen, sich auszuruhen. Es gibt noch große Unterschiede zwischen den Einrichtungen, wann ein betrieblicher Datenschutzbeauftragter wie einbezogen wird und mit welchem zeitlichen Budget er welche Aufgabe erledigen kann.

Neben der Benennung eines betrieblichen Datenschutzbeauftragten sind die kirchlichen Einrichtungen auch verpflichtet, diese Person bei der Datenschutzaufsicht als betrieblichen Datenschutzbeauftragten zu melden. Die Meldung kann beim Katholischen Datenschutzzentrum elektronisch über ein Meldeportal[6] abgegeben werden. Dieser Weg wird gut angenommen und häufig genutzt.

Das Katholische Datenschutzzentrum hat im vergangenen Jahr jedoch festgestellt, dass noch nicht alle verpflichteten Einrichtungen ihrer Meldepflicht nachgekommen sind. Die Pflicht zur Benennung von betrieblichen Datenschutzbeauftragten ergibt sich aus § 36 KDG. Auf der Meldeplattform kann über die "Änderungsmeldung" eine gleichzeitige Ab- und Neuanmeldung eines betrieblichen Datenschutzbeauftragten vorgenommen werden.

An dieser Stelle wird darauf hingewiesen, dass die fehlende Benennung eines notwendig zu benennenden betrieblichen Datenschutzbeauftragten oder die unterlassene Meldung des benannten betrieblichen Datenschutzbeauftragten gegenüber der Datenschutzaufsicht Anordnungen nach § 47 KDG bis hin zur Verhängung eines Bußgeldes nach sich ziehen können.

6 Siehe https://www.katholisches-datenschutzzentrum.de/meldung-bdsb/

3.2 Das Betroffenenrecht auf Auskunft

Gemäß den §§ 17 bis 25 KDG stehen einer betroffenen Person zahlreiche Rechte zu, wenn es um die Verarbeitung ihrer personenbezogenen Daten geht. Neben den Pflichten des Verantwortlichen normiert das KDG somit auch die Rechte der betroffenen Person und stärkt ihre rechtlichen Möglichkeiten in Bezug auf die Verarbeitung der personenbezogenen Daten.

Im KDG finden sich vor den Rechten der betroffenen Person mit den §§ 14 bis 16 KDG die Informations- und Transparenzpflichten des Verantwortlichen. Systematisch kann dies so zu verstehen sein, dass einige der darauffolgenden Rechte der betroffenen Person bereits im Vorfeld durch den Verantwortlichen bei der Wahrnehmung seiner rechtlichen Pflichten „erledigt" werden könnten. Ein großes Ziel des Datenschutzes sollte immer die Transparenz im Umgang mit der Verarbeitung personenbezogener Daten sein.

Durch die im Berichtszeitraum an das Katholische Datenschutzzentrum gerichteten Anfragen oder Beschwerden wurde bestätigt, dass das zentrale Betroffenenrecht das Auskunftsrecht aus § 17 KDG ist. Gerade aufgrund dieser zentralen Funktion und der umfangreichen Regelung fällt es den Verantwortlichen schwer, den Auskunftsersuchen der Betroffenen immer gerecht zu werden. Nicht nur der Umfang, sondern auch die Frist innerhalb derer ein Auskunftsverlangen zu beantworten ist, bereiten in der Praxis oft Probleme, da die Einrichtungen auf derartige Anfragen teilweise noch nicht ausreichend vorbereitet zu sein scheinen. Dies lässt sich vor allem dadurch vermuten, dass die an das Katholische Datenschutzzentrum gerichteten Beschwerden zeigten, dass die Beschwerdeführer mit den Angaben der Verantwortlichen - sofern welche gemacht wurden - nicht zufrieden waren.

Schon die Feststellung der Identität der anfragenden Person ist der erste wichtige Schritt, da personenbezogene Daten nicht herausgegeben und damit keine Auskunft nach § 17 KDG erteilt werden darf, wenn die Identität der anfragenden Person nicht hinreichend sicher feststeht. Dies gilt insbesondere, wenn der Versand der Auskunft an eine andere, als die zum Kontakt hinterlegte (E-Mail-)Adresse gewünscht wird. Dabei ist von einer Antwort per unverschlüsselter E-Mail abzuraten, da die im Rahmen einer Auskunft zusammengetragenen Informationen sehr sensible Daten enthalten und zum Teil sehr umfangreich sein können. Auch bei der Beantwortung eines Auskunftsanspruches ist der Datenschutz zu wahren. Im Regelfall wird man aus einer Anfrage auf Auskunft nach § 17 KDG per E-Mail nicht schließen können, dass damit auch in eine Antwort mit umfangreichen und sensiblen Daten per unverschlüsselter E-Mail eingewilligt worden ist. Dies befreit den Verantwortlichen jedoch nicht von seiner Pflicht, die Auskunft zu erteilen, wenn es sich um eine berechtigte Anfrage handelt. Vielmehr muss der Verantwortliche in angemessener Weise die Identität der anfragenden Person verifizieren.

Ebenso wichtig ist die Einhaltung der gesetzlich vorgeschriebenen Frist. In § 14 Abs. 3 Satz 1 KDG ist geregelt, dass der Verantwortliche der betroffenen Person die Informationen innerhalb eines Monats

nach Eingang des Antrags zur Verfügung stellen muss. Zwar kann diese Frist um weitere zwei Monate verlängert werden, dies ist jedoch nur unter Berücksichtigung der Komplexität und der Anzahl von Anträgen möglich. Zusätzlich ist die Verlängerung von zwei Monaten nur möglich, wenn der Verantwortliche diese Verlängerung innerhalb eines Monats nach Eingang des Antrags gegenüber der betroffenen Person unter Angabe der Gründe geltend macht (vgl. § 14 Abs. 3 Satz 2 und 3 KDG). Dies bedeutet, dass die Frist zur Beantwortung der Anträge generell einen Monat und nur in Ausnahmefällen bis zu drei Monate beträgt.

Da die Rechte der Betroffenen in den §§ 17-24 KDG die Position des Einzelnen stärken und eine möglichst transparente Verarbeitung personenbezogener Daten hervorbringen sollen, ist es die Pflicht der Verantwortlichen, die Bearbeitung der Anträge der betroffenen Personen entsprechend sicherzustellen.

3.3 Auftragsverarbeitung und das andere Rechtsinstrument

Bei einer Auftragsverarbeitung verarbeitet der Auftragsverarbeiter, der eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle sein kann, die personenbezogenen Daten im Auftrag des Verantwortlichen[7]. Dabei erfolgt die Verarbeitung durch einen Auftragsverarbeiter gemäß § 29 Abs. 3 KDG auf Grundlage eines Vertrages oder eines anderen Rechtsinstruments nach dem kirchlichen Recht, dem Recht der Europäischen Union oder dem Recht ihrer Mitgliedstaaten, der beziehungsweise das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet.

Auch in den Fällen, wo eine kirchliche Stelle eine (Dienst-)Leistung für eine andere kirchliche Stelle erbringt, muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden, wenn die Voraussetzungen einer Auftragsverarbeitung vorliegen. Der Charakter als rein innerkirchlicher Austausch der (Dienst-)Leistung, z.B. zwischen zwei selbständigen Pfarrgemeinden, entbindet nicht von der Notwendigkeit, einen Auftragsverarbeitungsvertrag abzuschließen.

In den Fällen, wo ein Auftragsverarbeiter eine gleichartige (Dienst-) Leistung einer Vielzahl von Kunden anbietet, kann es eine Erleichterung mit sich bringen, wenn dieser die Möglichkeit des „anderen Rechtsinstruments“ nutzt. Denn neben einer vertraglichen Regelung kann die Auftragsverarbeitung auch durch ein „anderes Rechtsinstrument“ begründet werden.

Dabei setzt ein „anderes Rechtsinstrument“ einen „gesetzlichen Rechtsakt“ voraus[8]. Dies kann eine EU-Verordnung, eine EU-Richtlinie oder ein nationales formelles Gesetz sein[9]. Da sich das in § 29 Abs. 3 KDG

7 Vgl. Definition des Auftragsverarbeiters in § 4 Nr. 8 KDG.
8 Vgl. zur parallelen Vorschrift der DS-GVO: Martini in Paal/Pauly, DSGVO/BDSG, 2. Aufl. 2018, Art. 28 Rn. 26.
9 Vgl. zur parallelen Vorschrift der DS-GVO: Bertermann in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 28 Rn 17 und Kremer in Schwartmann u.a., HK-DS-GVO/BDSG, 1. Aufl. 2018, Art. 28 Rn. 88.

im Vergleich zu Art. 28 Abs. 3 DSGVO zusätzlich eingefügte „andere Rechtsinstrument nach dem kirchlichen Recht“ an den Voraussetzungen der gleichzeitig genannten EU-Regelungen oder nationalen formellen Gesetzen orientieren muss, um die Gleichwertigkeit nach Art. 91 Abs. 1 DSGVO zu gewährleisten, hat der kirchliche Gesetzgeber mit dem „Gesetz zur Regelung des Rechtsinstruments nach § 29 Gesetz über den Kirchlichen Datenschutz (KDG)“ (§ 29-KDG-Gesetz) eine den oben genannten formellen Gesetzen auf europäischer oder nationaler Ebene gleichwertige formelle kirchliche Regelung geschaffen.

Dieses § 29-KDG-Gesetz gibt aber nur den Rahmen für die eigentlichen Regelungen der konkreten Auftragsverarbeitungen vor.

Die Regelungen des „anderen Rechtsinstruments“ müssen - wie bei einem Auftragsverarbeitungsvertrag - auf den konkreten Sachverhalt abgestimmt sein. Es müssen nach der DSGVO und dem KDG nicht mehr die konkreten technisch-organisatorischen Maßnahmen im Vertrag genannt werden, sondern der Vertrag oder das „andere Rechtsinstrument“ muss gemäß § 29 Abs. 4 Buchst. c) KDG vorsehen, dass der Dienstleister „alle gemäß § 26 KDG erforderlichen Maßnahmen ergreift“. Das § 29-KDG-Gesetz sieht zur Regelung dieser konkreten Sachverhalte in § 3 des Gesetzes eine Ermächtigung des Generalvikars zum Erlass von Verwaltungsverordnungen vor.

Die Mindestvorgaben, die das „andere Rechtsinstrument“ inhaltlich abdecken muss, sind nach § 29 Abs. 3 und 4 KDG identisch mit denen eines Auftragsverarbeitungsvertrages. Damit muss das „andere Rechtsinstrument“ für den konkreten Sachverhalt gemäß § 29 Abs. 3 KDG Festlegungen zum Gegenstand der Verarbeitung, der Dauer der Verarbeitung, Art und Zweck der Verarbeitung, der Art der personenbezogenen Daten, den Kategorien betroffener Personen und den Pflichten und Rechten des Verantwortlichen enthalten. Auch die weiteren Pflichten des Auftragsverarbeiters nach § 29 Abs. 4 KDG, wie z.B. die notwendigen technisch-organisatorischen Maßnahmen im Rahmen der Auftragsverarbeitung zu ergreifen (vgl. § 29 Abs. 4 Buchst. c) KDG), müssen durch das „andere Rechtsinstrument“ geregelt werden, auch wenn die konkret zu ergreifenden technisch-organisatorischen Maßnahmen nicht mehr zwingend im Auftragsverarbeitungsvertrag und damit auch im „anderen Rechtsinstrument“ zu benennen sind.

Aus dem Zusammenspiel zwischen § 29-KDG-Gesetz und der konkreten Verordnung ergibt sich die rechtliche Grundlage für eine Auftragsverarbeitung. Dabei ist zu beachten, dass eine Verordnung eben immer einen Sachverhalt eines Vertrages zur Auftragsverarbeitung ersetzen kann. Eine Sammelverordnung, die in einem Abschnitt alle möglichen Auftragsverarbeitungen erfassen will, wird die vorgenannten gesetzlichen Bedingungen des „anderen Rechtsinstruments“ nur schwer erfüllen. Es spricht aber nichts dagegen, verschiedene Sachverhalte in einem eigenen Abschnitt zu regeln und formal in einer Verordnung nach dem § 29-KDG-Gesetz zusammenzufassen. Dann wäre aber jeder Sachverhalt, der einen Auftragsverarbeitungsvertrag ersetzen soll, einzeln und vollständig für sich in einem getrennten Abschnitt dieser Verordnung nach dem § 29-KDG-Gesetz geregelt.

3.4 Cloud-Nutzung durch kirchliche Stellen

Viele kirchliche Stellen prüfen im Rahmen einer Aktualisierung ihrer IT-Infrastruktur, ob ein Wechsel in die „Cloud" nicht organisatorisch und wirtschaftlich sinnvoll ist. Unter diesem Schlagwort verbergen sich bei genauerer Betrachtung jedoch eine Vielzahl sehr unterschiedlicher Funktionen und technischer Varianten. In der Bandbreite zwischen den selbst betriebenen Rechenzentren, der Nutzung gemieteter Infrastruktur und Plattformen, bis hin zur Anmietung von verschiedenen Dienstleistungen einer bestehenden Softwarelösung, sind die zu klärenden datenschutzrechtlichen Fragen sehr unterschiedlich.

In vielen Fällen betreiben die kirchlichen Einrichtungen kein eigenes Rechenzentrum, sondern nutzen die Kapazitäten eines Dienstleisters. Die vertragliche Klärung der Datensicherheit, des Datenschutzes und der Vertraulichkeit der Einrichtungsdaten sind bei der Nutzung externer Dienstleister zentrales Kernthema. Regelungen hierzu finden sich zum einen in dem abzuschließenden Dienstleistungsvertrag und zum anderen in dem notwendigerweise erforderlichen Auftragsverarbeitungsvertrag.

Im Rahmen des Auftragsverarbeitungsvertrages ist entscheidend, ob es sich um einen Dienstleister handelt, der die Daten im Inland oder EU-Ausland verarbeitet oder die Datenverarbeitung außerhalb der EU-Grenzen stattfindet. Innerhalb von Deutschland und dem EU-Ausland gelten flächendeckend die gleichen Datenschutzregelungen, so dass hier gemäß § 29 Abs. 11 KDG eine Verarbeitung stattfinden darf. Die Verarbeitung in Drittstaaten ist jedoch nur zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission gemäß § 40 Abs. 1 KDG vorliegt oder wenn die Datenschutzaufsicht selbst oder eine andere Datenschutzaufsicht feststellt, dass dort ein angemessenes Datenschutzniveau vorliegt. Das Privacy Shield Abkommen der EU mit den Vereinigten Staaten stellt grundsätzlich nach § 29 KDG ein solches Abkommen dar und ermöglicht die Nutzung von US-amerikanischen Dienstleistern, die sich zu diesem Abkommen verpflichtet haben. Das Privacy Shield Abkommen wird jedoch momentan in einem gerichtlichen Verfahren vor dem EuGH überprüft. Es gilt als wahrscheinlich, dass dieses Abkommen wie seine Vorgänger auch nicht in der aktuell gültigen Version bestehen bleibt.

Die Nutzung von Cloud Produkten US-amerikanischer Anbieter ist aus zwei voneinander unabhängigen Richtungen mit Risiko behaftet. Zum einen ist nicht bei allen Produkten geklärt, inwieweit Daten an den Anbieter zurückfließen und zu welchem konkreten Zweck diese dort weiterverarbeitet werden. Zum anderen ermöglicht die US-amerikanische Gesetzgebung den Geheimdiensten und Strafverfolgungsbehörden den Zugriff auf alle gespeicherten Daten sämtlicher Kunden US-amerikanischer Firmen (Clarifying Lawful Overseas Use of Data-Act).

Bei der Bewertung der Risiken müssen alle Einrichtungen unabhängig von dem ausgewählten Anbieter die oben erwähnten Grundrisiken mit bewerten und wenn der Einsatz der Produkte für die Einrichtung unverzichtbar ist, Strategien entwickeln, wie trotzdem ein datenschutzkonformer Betrieb möglich ist.

3.5 Einzelfragen zu Meldungen an die Datenschutzaufsicht nach § 33 KDG

In der Praxis der Datenschutzaufsichten stellen die Meldungen an die Datenschutzaufsicht nach § 33 KDG einen nicht unerheblichen Anteil an den zu bearbeitenden Sachverhalten dar. Da eine unterlassene oder fehlerhafte Meldung einen Verstoß gegen das KDG darstellt und damit von der Datenschutzaufsicht auch geahndet werden kann, erreichen das Katholische Datenschutzzentrum viele Anfragen zur Anwendung des § 33 KDG.

Umfang der Meldepflicht gemäß § 33 Abs. 4 KDG

Es kommt immer wieder vor, dass Meldungen nicht rechtzeitig abgegeben werden, weil zum Zeitpunkt des Fristablaufs noch nicht sämtliche Informationen vorliegen.

Diese Situation hat der Gesetzgeber schon berücksichtigt und eine Lösung mit der Regelung des § 33 Abs. 4 KDG bereitgestellt. Informationen, die zum Zeitpunkt des Fristablaufs nach § 33 Abs. 1 KDG noch nicht vorliegen, können gemäß dieser Regelung nachgereicht werden, sobald dies der Fall ist.

Durch diese gesetzliche Regelung wird dem Umstand Rechnung getragen, dass sich komplizierte Sachverhalte nicht immer kurzfristig vollumfänglich klären lassen.

Sinn und Zweck der kurzen Meldefrist nach § 33 KDG ist, dass hier der Aufsicht die Möglichkeit gegeben werden soll, bei hohen Risiken für die Rechte und Freiheiten der betroffenen Personen schnellstmöglich einzuschreiten. Das Nachholen der noch offenen Informationen kann formlos erfolgen.

Einhaltung der 72-Stunden-Frist

Das Katholische Datenschutzzentrum hat festgestellt, dass die 72-Stunden-Meldefrist in vielen Fällen nicht eingehalten wird. Teilweise wurde die Meldefrist um mehrere Wochen überschritten.

Die Ursachen hierfür sind vielfältig. Am häufigsten wurde als Grund für die Verzögerung angegeben, dass die intern Verantwortlichen oder der betriebliche Datenschutzbeauftragte in Urlaub gewesen seien beziehungsweise, dass die Einrichtung im zeitlichen Zusammenhang mit Feiertagen personell nur gering besetzt gewesen sei. Vor dem Hintergrund des Schutzzwecks dieser Frist können diese Gründe keine Entschuldigung für eine derartige Überschreitung der gesetzlichen Meldefrist sein. Hier müssen die kirchlichen Einrichtungen durch interne Organisationsmaßnahmen sicherstellen, dass Datenschutzverletzungen auch in diesen Fällen gemeldet werden. Grundlage für diese Feststellung ist der erweiterte Schutzzweck der Normen § 33 und § 34 KDG. Die frühzeitige und umfassende Information der Datenschutzaufsicht dient unter anderem dazu, dass die Datenschutzaufsicht auf Grundlage der gemeldeten Verstöße die Möglichkeit hat, frühzeitig auf die Ergrei-

fung von Gegenmaßnahmen hinzuwirken. Sofern die betroffenen Personen nach § 34 KDG zu informieren sind, soll ihnen durch die zeitnahe Information ermöglicht werden, eventuell selbst noch Maßnahmen zu ergreifen, um die Folgen der Datenschutzverletzung abzumildern.

Kommt der Verantwortliche in der nach § 33 KDG notwendigen Risikobewertung zunächst zu dem Ergebnis, dass keine Meldepflicht vorliegt und ändert er nach Bekanntwerden weiterer Umstände der Datenschutzverletzung seine Risikoeinschätzung nachträglich, so ist die Meldung unverzüglich nachzuholen.

Konsequenzen

Bisher wurden die jeweiligen Einrichtungen auf die verfristete Meldung hingewiesen und zur Überarbeitung des internen Prozesses aufgefordert. Nach Inkrafttreten des KDG im Mai 2018 kann nunmehr davon ausgegangen werden, dass die Meldeprozesse in den einzelnen Einrichtungen mittlerweile implementiert sind. Aus diesem Grund wird das Katholische Datenschutzzentrum ab Januar 2020 bei Verstößen gegen die Meldefrist genau prüfen, ob im Einzelfall Maßnahmen nach § 47 und § 51 KDG angebracht erscheinen. Die Maßnahmen werden abhängig von der Dauer der Verfristung und von den angegebenen Verspätungsgründen angeordnet werden.

3.6 Einwilligung in schlechtere technische und organisatorische Maßnahmen

In mehreren Fällen wurde die Problematik an das Katholische Datenschutzzentrum herangetragen, dass Betroffene aufgefordert worden sind, in Verarbeitungen einzuwilligen, deren technische und organisatorischen Maßnahmen nicht den Voraussetzungen des KDG und der KDG-DVO entsprachen. So wurden sie z.B. aufgefordert, in eine unverschlüsselte E-Mail-Kommunikation bei der Verarbeitung von Gesundheitsdaten einzuwilligen.

Während sonst die Einwilligung überhaupt erst die Verarbeitung der Daten als Rechtsgrundlage nach § 6 Abs. 1 lit. b) KDG ermöglichen soll, wird sie in diesen Fällen dazu genutzt, um bei einer schon aus anderen Gründen bestehenden Erlaubnis zur Verarbeitung der personenbezogenen Daten von den im KDG und der KDG-DVO vorgesehenen Schutzmaßnahmen abzuweichen. Dieses Vorgehen hält das Katholische Datenschutzzentrum für kritisch.

Das kirchliche Datenschutzrecht sieht in § 26 KDG vor, dass der Verantwortliche dem Risiko der konkreten Verarbeitung personenbezogener Daten angemessene technische und organisatorische Schutzmaßnahmen trifft. Davon kann er sich nicht dadurch befreien, dass er die betroffene Person in eine Verschlechterung des Schutzes der Daten einwilligen lässt. Hier mag sich im Einzelfall sogar die Frage stellen, ob noch die für eine Einwilligung notwendige Freiwilligkeit vorliegt, wenn der Verarbeiter der Daten deutlich macht, dass eine Erbringung der gewünschten Leistung nur möglich ist, wenn diese Einwilligung erteilt wird.

Die Konferenz der Diözesandatenschutzbeauftragten hat dieses Thema aufgegriffen und dazu einen Beschluss im Sinne der oben dargestellten Argumentation gefasst[10].

Für die Praxis bedeutet dieser Beschluss, dass die katholischen Datenschutzaufsichten derartig erteilte Einwilligungen nicht als wirksame Grundlage einstufen, um von den nach § 26 notwendigen technischen und organisatorischen Schutzmaßnahmen bei der Verarbeitung personenbezogener Daten abzuweichen.

Das KDG gilt für die kirchlichen Einrichtungen dabei nicht nur in ihrer Position als Verantwortlicher, der die Daten verarbeitet, sondern insbesondere auch in den Fällen, in denen ihre Daten durch Vertragspartner verarbeitet werden, die den staatlichen Datenschutzregelungen unterliegen. Von kirchlichen Einrichtungen in diesen Vertragsverhältnissen erteilte Einwilligungen zu einer Datenverarbeitung mit schlechteren technischen und organisatorischen Schutzmaßnahmen werden von den kirchlichen Datenschutzaufsichten daher ebenfalls als unwirksam angesehen und können gegebenenfalls einen meldepflichtigen Datenschutzverstoß darstellen.

3.7 Gemeinsame Verantwortlichkeit

Mit mittlerweile drei Entscheidungen[11] hat der Europäische Gerichtshof den Blick auf eine Vorschrift in der DSGVO gelenkt, die bisher nicht im Fokus der meisten Anwender stand. Auch wenn diese Entscheidungen noch zur bis 2018 anwendbaren europäischen Richtlinie zum Datenschutz ergangen sind, ist aufgrund der vergleichbaren Begrifflichkeiten der alten Richtlinie und der jetzt geltenden DSGVO davon auszugehen, dass diese Urteile auch für die DSGVO anwendbar sind.

In Art. 26 DSGVO sind die Vorgaben für die gemeinsame Verantwortlichkeit bei der Verarbeitung personenbezogener Daten festgeschrieben. Diese Regelung wurde in § 28 KDG in sprachlich leicht veränderter Form übernommen.

Der EuGH legt in seinen Urteilen den Begriff der gemeinsamen Verantwortlichkeit weit aus, um einen umfassenden Schutz der betroffenen Personen zu erreichen. Dabei stellt das Gericht auf den Beitrag zur Entscheidung der einzelnen Beteiligten über die Mittel und Zwecke der Verarbeitung ab. Diese Beiträge müssen nicht gleich gewichtet sein. Diese Beiträge beziehungsweise die Verantwortlichkeiten für die Datenverarbeitung können sich in verschiedenen Phasen der Verarbeitung unterscheiden und eventuell auch begrenzt sein.

Bei der gemeinsamen Entscheidung über die Mittel der Verarbeitung sieht es das Gericht als ausreichend an, dass der Internetseitenbetreiber z.B. mit der Platzierung eines Social-Media-Plugins auf seiner Seite dem Social-Media-Anbieter die Datenerhebung ermöglicht und

10 Der Beschluss ist abgedruckt im Abschnitt 5.2.4 dieses Jahresberichts.

11 Urteil vom 05.06.2018 (Rs. C-210/16 – Facebook-Fanpages); Urteil vom 10.07.2018 (Rs. C-25/17 – Zeugen Jehovas) und Urteil vom 29.07.2019 (Rs. C-40/17 – Fashion-ID). Zum Urteil vom 29.07.2019 (Fashion-ID) siehe auch Abschnitt 2.1.1 dieses Jahresberichtserichts.

damit über die Mittel der Verarbeitung – das Plugin – mitentscheidet. Auch bei dem gemeinsamen Zweck der Verarbeitung muss keine Identität des Zwecks vorliegen. Es ist nach Ansicht des EuGHs ausreichend, wenn sich die Zwecke der Beteiligten ergänzen und so beide das gleiche Ziel verfolgen.

Auch wenn die Urteile des EuGHs in Detailfragen noch Raum für Auslegungsfragen bieten, so hat das Gericht die Richtung an dieser Stelle deutlich vorgegeben.

Die kirchlichen Einrichtungen sollten daher ihre Verarbeitungen personenbezogener Daten daraufhin überprüfen, ob eine gemeinsame Verantwortlichkeit vorliegen könnte. Diese Überprüfung hatte das Katholische Datenschutzzentrum bezogen auf die Facebook-Fanpages schon im letzten Bericht angeregt[12].

Im Rahmen der Überprüfung auf eine mögliche gemeinsame Verantwortlichkeit sollte zuerst der eigene Anteil an der Verarbeitung bestimmt werden. Dabei sind die Mittel und Zwecke der Verarbeitung ebenso zu betrachten wie die Rechte und Pflichten, die die kirchliche Stelle im Rahmen der Verarbeitung vertraglich eingeht. In einem zweiten Schritt sollte dann der Anteil der weiteren Beteiligten nach den gleichen Maßstäben bestimmt werden.

Kommt die kirchliche Einrichtung nach diesen Überlegungen zu dem Schluss, dass eine gemeinsame Verantwortlichkeit im Sinne des § 28 KDG besteht, muss sie sich um die Erfüllung der in § 28 KDG genannten Pflichten kümmern. Dazu ist nach § 28 Abs. 1 Satz 2 KDG erforderlich, dass die gemeinsam Verantwortlichen in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtungen gemäß diesem Gesetz erfüllt, insbesondere wer den Informationspflichten gemäß den §§ 15 und 16 nachkommt. § 28 Abs. 2 regelt ergänzend, dass die Vereinbarung gemäß Absatz 1 die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber der betroffenen Person enthält. Außerdem ist die betroffene Person über den wesentlichen, die Verarbeitung personenbezogener Daten betreffenden Inhalt der Vereinbarung zu informieren.

Bei der Ausgestaltung einer solchen gemeinsamen Verantwortlichkeit ist auch zu beachten, dass gemäß § 28 Abs. 3 KDG, ungeachtet der Einzelheiten der Vereinbarung gemäß § 28 Abs. 1 KDG, die betroffene Person ihre Rechte im Rahmen des KDG bei und gegenüber jedem Einzelnen der Verantwortlichen geltend machen kann. Dies bedeutet im Umkehrschluss, dass auch jeder beteiligte Verantwortliche diese Verpflichtungen erfüllen können muss.

12 Siehe Abschnitt 3.5.8 im Jahresbericht 2018 des Katholischen Datenschutzzentrums.

3.8 Thematische Schwerpunkte bei Meldungen nach § 33 KDG

Im Berichtsjahr war ein erheblicher Anstieg der Zahl der abgegebenen Meldungen nach § 33 KDG zu verzeichnen. Im Vergleich zum zweiten Halbjahr 2018 (dem ersten Halbjahr nach Inkrafttreten des KDG) stieg die Zahl der Meldungen von Datenschutzverletzungen im ersten Halbjahr 2019 um 50 Prozent, im zweiten Halbjahr hatte diese sich sogar verdoppelt. Der Anstieg ist aus Sicht des Katholischen Datenschutzzentrums auf eine gestiegene Sensibilität bei der Erkennung von Datenschutzverstößen, die aufmerksame Arbeit vieler betrieblicher Datenschutzbeauftragter und den mittelfristig eingetretenen Erfolg vieler Informations- und Schulungsveranstaltungen zurückzuführen.

Trotz unterschiedlichster Thematiken lassen sich Schwerpunkte bilden.

Unberechtigtes Offenlegen von Gesundheitsdaten

Besonders in Einrichtungen der Gesundheitsfürsorge kam es gehäuft zur unbefugten Offenlegung von Gesundheitsdaten gegenüber Dritten durch Fehlversand von Unterlagen. Häufigstes Beispiel ist der Faxfehlversand von Kranken-, Befund- oder Entlassberichten. Aber auch ein Fehlversand auf dem Postweg oder die unbefugte Offenlegung nur durch die Übergabe eines Berichtes an einen falschen Patienten waren Inhalte der gemeldeten Datenschutzverletzungen nach § 33 KDG.

„... die Sorgfältigkeit der Mitarbeitenden spielt eine zentrale Rolle bei dem Umgang mit personenbezogenen Daten ...“

Gerade im Umgang mit Gesundheitsdaten als personenbezogene Daten der besonderen Kategorie (vgl. § 4 Nr. 2 und Nr. 17 KDG) ist der Schutz dieser Daten eine Pflicht des Verantwortlichen, welche durch unzureichende technische und organisatorische Maßnahmen nicht vernachlässigt werden darf. Auch die Sorgfältigkeit der Mitarbeitenden spielt eine zentrale Rolle bei dem Umgang mit personenbezogenen Daten der besonderen Kategorie. Von Seiten der Einrichtungen müssen Schutzmaßnahmen ergriffen werden, um auch in einem stressigen Klinikalltag zu verhindern, dass eine falsche Ziffer in das Faxgerät getippt oder versehentlich zwei Befundberichte zu unterschiedlichen Patienten an einen Adressaten geschickt werden. Dies sind Beispiele für datenschutzrechtlich relevante Fälle, wie sie sich im Berichtsjahr gehäuft ereignet haben. Je nach der Art der Offenlegung und der Kritikalität der Gesundheitsdaten kann es sich in diesen Fällen um einen großen Eingriff in das allgemeine Recht auf informationelle Selbstbestimmung der betroffenen Person handeln. Da den Sachverhalten oftmals vermeidbare Fehler von Mensch oder Technik zugrunde liegen, hofft das Katholische Datenschutzzentrum, dass sich durch fortlaufend durchgeführte Sensibilisierungsmaßnahmen der Mitarbeitenden und Weiterentwicklung technischer Schutzmaßnahmen im kommenden Jahr eine positivere Bilanz ziehen lassen wird.

Abhandenkommen von Datensätzen in Kindertageseinrichtungen

Die weitaus größte Zahl von Meldungen betraf den Verlust und die gleichzeitige potentielle Offenlegung von Daten im Zusammenhang mit Einbruchdiebstählen von Computern, Laptops, Mobiltelefonen und Kameras, besonders aus Kindertageseinrichtungen. Eine

unzureichende physische Zutrittssicherung (z.B. mangelhafter Einbruchsschutz an Fenstern und Türen) verbunden mit organisatorischen Versäumnissen (z.B. kein Backup der Daten, Speicherung auf lokalen Datenträgern anstatt in Rechenzentren) und vor allem die Vernachlässigung der verbindlichen Vorgaben des § 26 KDG und der KDG-Durchführungsverordnung zu den technischen und organisatorischen Schutzmaßnahmen für die personenbezogenen Daten (z.B. Verschlüsseln von sensiblen personenbezogenen Daten) führte in mehr als 100 Fällen zu der Situation, dass nicht nur das wertvolle Inventar (Hardware) gestohlen wurde, sondern auch den betroffenen Eltern zu berichten war, dass z.B. Daten über den Bildungsstand der Kinder, persönlicher Schriftverkehr oder Kontodaten in unbefugte Hände gelangt waren.

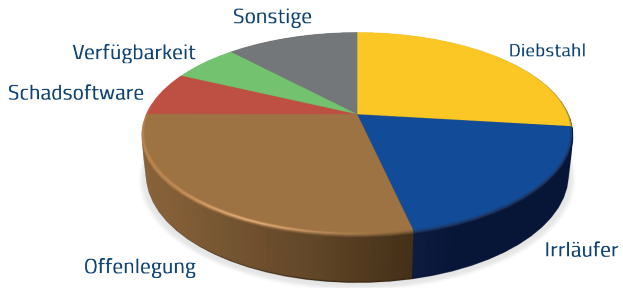
Wegen der enormen Häufung dieser Vorfälle hat das Katholische Datenschutzzentrum zu dieser Problematik erläuternde Artikel in Fachzeitschriften für Kindertageseinrichtungen veröffentlicht und schließlich eine Querschnittsprüfung[13] in seinem Zuständigkeitsgebiet angestoßen.

Malware

Eher selten wurden Vorfälle gemeldet, bei denen es zu Störungen und Verletzungen des Schutzziels der Verfügbarkeit durch den Befall mit Schadsoftware (z.B. Viren oder Trojaner) gekommen ist. Vermutlich haben Verantwortliche oft eine Meldung in diesen Fällen unterlassen, weil sie nach der notwendigen Risikobewertung des Sachverhaltes keine Gefährdung der Rechte und Freiheiten natürlicher Personen angenommen haben.

In den gemeldeten Fällen sind meistens E-Mail-Adressen durch einen Trojaner ausgelesen und anschließend für Spam-Mail- oder Phishing-Aktionen missbraucht worden. Auch zu irreversiblen Verschlüsselungen ganzer Server und Netzwerke ist es vereinzelt gekommen, wodurch der jeweiligen Organisation hoher Schaden entstanden ist, da die IT-Struktur oft mit viel Personalaufwand neu aufzubauen war.

Meldungen von Datenschutzverletzungen



Erläuterung:
Diebstahl: Entwendung von Hardware mit unverschlüsselten Daten; *Irrläufer*: Korrekter Datenübermittlungsprozess, aber (menschlicher) Fehler bei Auswahl des Datenempfängers; *Offenlegung*: Unzulässiger Datenübermittlungsprozess, versehentlich oder vorsätzlich durchgeführt; *Schadsoftware*: z.B. fremdgesteuerter Zugriff auf Email-Kontakte, Verschlüsselung von Dateien; *Verfügbarkeit*: Defekt eines Datenträgers oder versehentliche Löschung, ohne Backup und Wiederherstellmöglichkeit.

13 Siehe Abschnitt 3.11 dieses Jahresberichts.

3.9 Thematische Schwerpunkte bei Beschwerden

Im Berichtsjahr wandten sich zahlreiche Betroffene mit datenschutzrechtlich relevanten Beschwerden an das Katholische Datenschutzzentrum. Gemäß § 48 Abs 1 KDG steht dies jeder betroffenen Person zu.

Personenbezogene Daten von Spendern

Im Zusammenhang mit der Sammlung von Sach- oder Geldspenden werden, zur Verbuchung der Spenden oder um die Spender bei erneuten Aktionen kontaktieren zu können, die personenbezogenen Daten der Spender gespeichert.

Durch mehrere Beschwerden wurde das Katholische Datenschutzzentrum im Berichtszeitraum darauf aufmerksam, dass diese Listen der Spender nicht immer datenschutzrechtlich korrekt geführt beziehungsweise genutzt werden. Gerade wenn ein Spender ausdrücklich der weiteren Verwendung seiner Adressdaten widerspricht, ist dies zu respektieren und es besteht rechtlich keine Möglichkeit, ihm trotzdem Werbung beziehungsweise Informationen zu erneuten Spendenaktionen zukommen zu lassen. Den entsprechenden Stellen ist somit auferlegt, dass sie die vorhandenen Spenderdaten ganz eindeutig separieren, so dass es nicht zur unberechtigten Kontaktaufnahme mit Spendern kommt, die einer solchen widersprochen haben. Die Speicherung der Spenderdaten in den gesetzlich geforderten Fällen (z.B. nach Steuerrecht) bleibt davon unberührt.

„Die Bearbeitung der Beschwerden hat gezeigt, dass durch einfache technische und organisatorische Maßnahmen Datenschutzverletzungen verhindert ... werden können. “

Die Bearbeitung der Beschwerden hat gezeigt, dass durch einfache technische und organisatorische Maßnahmen Datenschutzverletzungen verhindert und damit Beschwerden vorgebeugt werden können.

Fehlversand von Patientenunterlagen

Ebenso wie bei den Meldungen von Datenschutzverletzungen gemäß § 33 KDG gab es zahlreiche Beschwerden von Patienten, welche den Umgang mit ihren Gesundheitsdaten monierten. Oftmals kam es zu einem Fehlversand von Arztberichten, weil im Krankenhausinformationssystem (KIS) ein nicht behandelnder Arzt eingetragen war, die erforderliche Einwilligung zur Weiterleitung an den Hausarzt nicht erteilt wurde, Befunde vertauscht oder durch einen Kuvertierfehler mehrere Datensätze versendet wurden. Gerade bei den Gesundheitsdaten und allgemein bei den personenbezogenen Daten der besonderen Kategorie ist das zu beachtende Schutzniveau besonders hoch anzusetzen, um die unbefugte Offenlegung möglichst zu vermeiden.

Unberechtigte Einsichtnahme in elektronische Patientendaten

In mehreren Fällen beschwerten sich betroffene Personen, dass während oder nach einem Krankenhausaufenthalt ihre im Krankenhausinformationssystem abgelegten Stamm- und Behandlungsdaten durch Mitarbeitende des Krankenhauses unberechtigt eingesehen, teilweise

kopiert und missbräuchlich verwendet wurden. In den meisten Fällen handelte es sich bei den Betroffenen selbst um Mitarbeitende des Krankenhauses oder Verwandte oder Bekannte der Mitarbeitenden, denen die unberechtigte Einsichtnahme vorgeworfen wurde.

In den Fällen, in denen die Beschwerde vom Katholischen Datenschutzzentrum als berechtigt eingestuft wurde, hatten die sich fehlverhaltenden Mitarbeitenden des Krankenhauses ihre prinzipiell richtig vorgegebenen Berechtigungen (z.B. in der Verwaltung zur Erstellung einer Abrechnung) im KIS zweckentfremdend verwendet, um z.B. private Interessen zu verfolgen. Dabei wurden zum Teil bestehende Dienstanweisungen verletzt. Die Fehlverhalten konnten meistens durch die im KIS voreingestellten Protokollierungen der Zugriffe auf die Patientendaten aufgedeckt werden.

Als Konsequenz wird das Katholische Datenschutzzentrum bei zukünftigen Prüfungen von Krankenhäusern und deren Informationssystemen verstärkt darauf achten, dass die Mitarbeitenden ausdrücklich auf die zweckgebundene Verarbeitung der Patientendaten geschult werden und dass Prozesse zur regelmäßigen Auswertung von Systemprotokollen zu kritischen Zugriffen implementiert sind.

3.10 Thematische Schwerpunkte bei Beratungen und Anfragen

Gemäß § 44 Abs. 3 lit. b) KDG hat eine Datenschutzaufsicht im Rahmen ihres Zuständigkeitsbereichs insbesondere auch die Aufgabe, kirchliche Einrichtungen und Gremien über Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung ihrer Daten zu beraten.

So kam es im Berichtszeitraum zu zahlreichen Anfragen durch betroffene Personen oder Einrichtungen, welche sich nicht sicher waren, wie sie mit einer bestimmten Verarbeitungstätigkeit rechtssicher umzugehen haben. Die Anzahl der Anfragen ist von ihrem sehr hohen Wert im Jahr 2018 im Jahr 2019 wieder etwas zurückgegangen. Vermutlich liegt dies vor allem an einer immer besseren Vor-Ort-Beratung durch die betrieblichen Datenschutzbeauftragten, die sehr dazu beitragen, Datenschutzfragen situationsgerecht und gesetzeskonform direkt am Ort ihrer Entstehung zu lösen.

Ließ sich im Jahr 2018 ein deutlicher Schwerpunkt der Anfragen im Bereich der Foto- und Videoaufnahmen verzeichnen, sind diese Anfragen 2019 deutlich zurückgegangen. Dies mag zum einen an den zur Verfügung gestellten Informationsblättern liegen, zum anderen daran, dass sich die anfänglich große Unsicherheit etwas gelegt hat. Gleichwohl ist die eigentliche Frage zu dem Umgang mit Fotos- und Videoaufnahmen und die damit verbundene Frage der Fortgeltung des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie noch nicht abschließend geklärt.

Im Berichtsjahr gab es vor allem Anfragen zu generellen Verarbeitungstätigkeiten, die durchaus von Relevanz für mehrere Einrichtungen waren. Zu nennen ist zum Beispiel das Konstrukt der gemeinsamen Verantwortlichkeit[14]. Dieses Rechtsinstrument gelangte erst durch die Urteile des EuGHs zur gemeinsamen Verantwortlichkeit in das Blickfeld einer größeren Öffentlichkeit.

Zu den „Klassikern" bei den Anfragen gehört nach wie vor die Frage nach einer Empfehlung zu Messenger-Produkten. Fast genauso oft wird nach der Zulässigkeit des Einsatzes privater (mobiler) Endgeräte zu dienstlichen Zwecken oder nach einer Bewertung konkreter Office365-Projekte gefragt.

Fragen nach einem datenschutzkonformen Messenger werden immer wieder dahingehend beantwortet, dass das Katholische Datenschutzzentrum keine direkten Produktempfehlungen geben und auch keine kontinuierliche Produktbewertung oder Marktbeobachtung leisten kann. Anhand der u.a. auf der Internetseite[15] veröffentlichten Kriterien kann jeder Verantwortliche auf Basis des von ihm konkret vorgesehenen Nutzungsszenarios selbst eine Risikobewertung (Datenschutzfolgenabschätzung) vornehmen.

Ähnlich werden Fragen zu Office365-Projekten beziehungsweise allgemeiner zu Cloud-Projekten beantwortet. Auch hier ist die individuelle Situation, insbesondere die betroffenen Datenkategorien und die sonstigen technischen und organisatorischen (Schutz-)Maßnahmen sowie die verfügbaren Alternativen, zu bewerten, bevor eine Risikobewertung der Speicherung personenbezogener Daten bei einem Fremdanbieter vollständig sein kann. Da es auch bei den angebotenen Lizenzmodellen bei Office365 hinsichtlich Ausgestaltung und Umfang und den datenschutzrechtlichen Zusicherungen von Microsoft an die Auftraggeber im Berichtsjahr Bewegungen gegeben hat, bleibt die Risikobewertung immer eine dynamische Aufgabe des Verantwortlichen und ist regelmäßig anzupassen[16].

Der Einsatz privater (mobiler) Endgeräte zu dienstlichen Zwecken wird in § 20 der KDG-DVO umfassend geregelt. Trotzdem erreichen das Katholische Datenschutzzentrum immer wieder Anfragen, weil die IT-Verantwortlichen der Einrichtungen vor sachlichen, organisatorischen oder finanziellen Herausforderungen stehen und mit dem Einsatz privater Endgeräte statt der Anschaffung dienstlicher Endgeräte versuchen, Investitionen zu vermeiden. Hier wurden die Einrichtungen unter Hinweis auf die Regelungen in der KDG-DVO und den geplanten Nutzungsszenarien oft auf die großen Schwierigkeiten des geplanten Einsatzes privater Geräte hingewiesen.

14 Siehe Abschnitt 3.7 dieses Jahresberichts.
15 Siehe https://www.katholisches-datenschutzzentrum.de/bewertung-von-messengerdiensten-aus-datenschutzsicht/
16 Siehe Abschnitt 3.4 dieses Jahresberichts.

3.11 Thematische Schwerpunkte bei Prüfungen, insbesondere die Querschnittsprüfung kirchlicher Kindertagesstätten

3.11.1 Prüfungen allgemein

Sofern ein Sachverhalt, von dem das Katholische Datenschutzzentrum Kenntnis erhält, hinreichende Anhaltspunkte für eine mögliche Verletzung des Schutzes personenbezogener Daten enthält, wird dieser Sachverhalt untersucht. Diese Prüfung findet im Regelfall im schriftlichen Verfahren statt, bei dem die Beteiligten angehört werden und dann eine Entscheidung auf Basis der vorliegenden Erkenntnisse getroffen wird.

Bedarf diese mögliche Verletzung des Schutzes personenbezogener Daten aus Sicht des Katholischen Datenschutzzentrums aufgrund der Beteiligten, der Art, des Umfangs oder der Folgen der Datenschutzverletzung oder anderer besonderer Umstände einer weitergehenden Betrachtung, so führt das Katholische Datenschutzzentrum auch Prüfungshandlungen vor Ort durch.

Neben diesen anlassbezogenen Prüfungen, bei denen ein der Datenschutzaufsicht zur Kenntnis gelangter Sachverhalt der Auslöser ist, führt das Katholische Datenschutzzentrum auch Prüfungen unabhängig von konkreten Sachverhalten durch. Diese anlasslosen Prüfungen sollen der Datenschutzaufsicht einen besseren Überblick über die Verarbeitung personenbezogener Daten in einem speziellen Themengebiet (z.B. Umsetzung technischer und organisatorischer Schutzmaßnahmen) und/oder einer Einrichtungsart (z.B. Kindertagesstätten) ermöglichen. Dieses Ziel kann durch die Prüfung einzelner Einrichtungen oder durch die Prüfung einer Stichprobe aus den Einrichtungen, wie das Katholische Datenschutzzentrum es bei der Querschnittsprüfung der Kindertagesstätten derzeit durchführt, erreicht werden.

Die Prüftätigkeit der Datenschutzaufsicht soll kein Selbstzweck sein. Vielmehr ist das Ziel der Prüfungstätigkeit ein durchschnittlich höheres Datenschutzniveau in der geprüften Zielgruppe zu schaffen und damit auch künftige Datenschutzverstöße zu verhindern.

In diesem Berichtszeitraum gab es nur vereinzelte Vor-Ort-Prüfungen. Die überwiegende Anzahl von Prüfungshandlungen konnte im schriftlichen Verfahren abgeschlossen werden.

3.11.2 Die Querschnittsprüfung kirchlicher Kindertagesstätten

Nachdem im Jahr 2018 aufgrund des sehr hohen Beratungsbedarfs durch das neue Datenschutzrecht keine anlasslosen Prüfungen durchgeführt wurden, sind diese im Jahr 2019 wieder aufgenommen worden. Zur Vorbereitung dieser Prüfungen wurde zunächst ermittelt, in welchen Bereichen die Schwerpunkte der gemeldeten Datenschutzverletzungen lagen.

„... Bedarf einer flächendeckenden Überprüfung des Schutzes dieser sensiblen Daten ... “

Die Auswahl der zu prüfenden Einrichtungen und des Prüfgegenstands erfolgte risikobasiert auf Basis der Auswertung der Meldungen hinsichtlich der Art der Datenschutzverletzungen und der betroffenen Einrichtungen. Es wurden uns häufig Datenschutzverletzungen gemeldet, bei denen Laptops, Fotoapparate oder mobile Datenträger (z.B. USB-Sticks oder SD-Karten) aus Kindertageseinrichtungen gestohlen wurden. Im Rahmen der Aufklärung der Sachverhalte stellte sich überwiegend heraus, dass die auf den Geräten vorhandenen Daten (z.B. Bildungsdokumentation, Berichte an Jugendämter und Fotos) ohne oder ohne ausreichenden Schutz gespeichert waren.

Hier ergab sich aus Sicht des Katholischen Datenschutzzentrums der Bedarf einer flächendeckenden Überprüfung des Schutzes dieser sensiblen Daten der den Kindertageseinrichtungen anvertrauten Kinder sowie deren Erzieher. Zur Erreichung dieses Ziels wurde das Instrument der Querschnittsprüfung gewählt, mit dem eine Vielzahl von Einrichtungen zu dem gleichen Sachverhalt befragt und geprüft werden kann.

Ein weiteres Kriterium für die Auswahl der Kindertagesstätten als Zielgruppe für die Prüfung war zudem, dass die Erhöhung des Datenschutzniveaus, in Bezug auf die dem Katholischen Datenschutzzentrum gemeldeten Sachverhalte, vor Ort mit einem geringen technischen Aufwand möglich ist. Durch die flächendeckende Auswahl besteht die Erwartung, dass die Themen Datenschutz im Allgemeinen und “Verschlüsselung“ im Besonderen in den Fokus der Verantwortlichen gerückt werden.

Das Katholische Datenschutzzentrum hat daher im Sommer 2019 alle Kindertageseinrichtungen in seinem Zuständigkeitsbereich mit einem Schreiben auf die Vorgaben zur technischen und organisatorischen Sicherung dienstlicher elektronischer Geräte, auf denen personenbezogene Daten gespeichert sind, hingewiesen und angekündigt, eine Querschnittsprüfung durchzuführen, die die Umsetzung des Schutzes der personenbezogenen Daten in den Kindertageseinrichtungen in diesem Bereich aufzeigen soll. Schwerpunkte sind dabei die Sicherung und Speicherung von Daten sowie der Aufbau der allgemeinen Datenschutzorganisation in den kirchlichen Einrichtungen.

Die eigentliche Querschnittsprüfung ist in mehrere Teilabschnitte aufgeteilt.

Der erste Teil besteht aus einem Fragebogen, der online ausgefüllt wird. Die Bearbeitungsfrist begann am 01.12.2019 und dauert bis zum 20.02.2020 an.

Im Anschluss an die stichprobenhafte Onlinebefragung und deren Auswertung sind als nächste Schritte eine erweiterte Dokumentenprüfung und im Anschluss stichprobenhafte Vor-Ort-Prüfungen vorgesehen.

Ziel dieses mehrstufigen Aufbaus ist es, ein möglichst präzises Bild von dem Implementierungsstand des Datenschutzes in den Kindertageseinrichtungen zu bekommen, ohne die Belastung für die einzelnen geprüften Einrichtungen zu hoch zu gestalten. So soll der Online-

Fragebogen als Einstieg dazu dienen, die Stärken und Schwächen der geprüften Einrichtung herauszufiltern. In den Bereichen, in denen die jeweilige Einrichtung den notwendigen Implementierungsgrad in den Antworten darstellt, kann von einer vertieften weiteren Prüfung abgesehen werden. Nur in den Teilbereichen, in denen möglicherweise noch Handlungsbedarf besteht, erfolgt eine Dokumentenprüfung. Auch in dieser Phase ist die Zielrichtung jedoch auf die Sensibilisierung der Verantwortlichen ausgerichtet und soll in erster Linie dazu dienen, notwendige technische und organisatorische Schutzmaßnahmen anzustoßen.

Nachdem im Sommer alle Kindertageseinrichtungen in katholischer Trägerschaft im Zuständigkeitsbereich des Katholischen Datenschutzzentrums mit dem Hinweis auf die geplante Querschnittsprüfung angeschrieben worden waren, wurden für die eigentliche Prüfung 101 Kindertageseinrichtungen als Stichprobe ausgewählt. Bei der Stichprobe wurde darauf geachtet, dass eine flächendeckende Verteilung auf die (Erz-)Diözesen gewährleistet ist.

Die Auswahl der konkreten Einrichtungen erfolgte nach dem Zufallsprinzip unter Berücksichtigung einer gleichmäßigen Verteilung in der Fläche.

Die Querschnittsprüfung wird in enger Kooperation mit dem Diözesandatenschutzbeauftragten für die Norddeutschen Bistümer durchgeführt, der für seinen Bereich zeitgleich ebenfalls eine Querschnittsprüfung der katholischen Kindertageseinrichtungen durchführt.

3.12 Umgang mit Kirchenbüchern, insbesondere durch Familienforscher

Das Katholische Datenschutzzentrum erhielt eine Anfrage durch eine Kirchengemeinde, unter welchen Umständen und in welchem Rahmen einem Familienforscher Zugriff auf die im Archiv der Kirchengemeinde verwahrten historischen Kirchenbücher gewährt werden müsse und ob der Person zu erlauben sei, Seiten der Kirchenbücher zu fotografieren.

Die Kirchengemeinde wurde auf die Bestimmungen der Kirchlichen Archivordnung hingewiesen, nach denen Kirchenbücher Sperrfristen unterliegen, die – im Fall von Taufbüchern – bis zu 120 Jahre (beginnend mit dem (Tauf-)Datum der letzten erfassten Person) betragen können. Der Zweck dieser Regelung ist es sicherzustellen, dass die Daten in den Kirchbüchern nach dieser Frist keine personenbezogenen Daten im Sinne des KDG mehr sind, da zu diesem Zeitpunkt alle verzeichneten Personen verstorben sein sollten.

Die Kirchengemeinde darf also nur Kirchenbücher zur Einsichtnahme bereitstellen, deren Sperrfrist abgelaufen ist. Alle jüngeren Kirchenbücher dürfen für einen Besucher des Archivs nicht verfügbar sein. Kopien, auch per Photographie, dürfen von den freigegebenen Büchern erlaubt werden. Es wurde der Kirchengemeinde empfohlen, ihr Vorgehen mit dem zuständigen Diözesanarchiv abzustimmen.

In der Anfrage einer anderen Kirchengemeinde ging es um allgemeine Nachforschungen, die ein der Kirchengemeinde bekannter Heimatforscher zur Geschichte des Ortes durchführen und dazu auch Einsicht in jüngere Kirchenbücher nehmen wollte. Bei einigen dieser Bücher war die Sperrfrist noch nicht abgelaufen. Es wurde der Kirchengemeinde mitgeteilt, dass es nach Einschätzung des Katholischen Datenschutzzentrums keine Rechtsgrundlage für einen Zugriff des Heimatforschers auf die jungen Kirchenbücher gäbe. Die Gemeinde hat den Heimatforscher dann als ehrenamtlichen Archivar mit der Sichtung und Ordnung des Gemeindearchivs beauftragt. Im Rahmen dieser Tätigkeit hat er Zugriff auf alle Archivmaterialien.

Zu beachten ist, dass diese Lösung nicht zu einer Umgehung der datenschutzrechtlichen und archivrechtlichen Vorgaben führen darf. Dem Mitarbeiter wird im Rahmen seiner neuen ehrenamtlichen Tätigkeit der Zugriff auf das Archivmaterial nur zu dienstlichen Zwecken gewährt. Eine private Verwertung seiner im Rahmen dieser Tätigkeit gewonnenen Erkenntnisse ist nur im Rahmen der gesetzlichen Vorgaben des Datenschutzes und des Archivrechts möglich.

Dementsprechend wurde mit ihm vereinbart, dass Erkenntnisse aus der Arbeit im Archiv vor einer Veröffentlichung oder anderer Verwertung durch die Kirchengemeinde freigegeben werden müssen.

4 Das Katholische Datenschutzzentrum

4.1 Zuständigkeitsbereich

Der Diözesandatenschutzbeauftragte und Leiter des Katholischen Datenschutzzentrums ist als Datenschutzaufsicht im Sinne des Art. 91 Abs. 2 DSGVO und der §§ 42 ff. KDG zuständig für die Erzdiözese Köln, die Erzdiözese Paderborn, die Diözese Aachen, die Diözese Essen und die Diözese Münster (nordrhein-westfälischer Teil). 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 Hessen, die zur Erzdiözese Paderborn gehören. In diesem Gebiet leben über 6,8 Millionen Menschen römisch-katholischen Glaubens (Stand 2018).

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 DDSB zuständig ist (Stand 2013). Darüber hinaus fallen noch diverse Vereine, Verbände und Stiftungen im kirchlichen Bereich in die Zuständigkeit des DDSB. Auch die Bundesverbände kirchlicher Vereinigungen, die ihren Sitz in Nordrhein-Westfalen haben, fallen aufgrund 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 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 (Erz-)Diözesen zusammengeschlossen. Neben dem Sekretariat der Deutschen Bischofskonferenz in Bonn gehören unter anderem die Geschäftsstelle des VDDs in Bonn, das Kommissariat der deutschen Bischöfe – Katholisches Büro in Berlin und weitere Einrichtungen des VDDs zum Zuständigkeitsbereich.

4.2 Aufbau der Einrichtung

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

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 wurde dem Leiter des Katholischen Datenschutzzentrums übertragen.

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

Dem DDSB sind ein Vertreter, Referenten, Sachbearbeiter und Sekretariatskräfte zur Seite gestellt, die auch vom Katholischen Datenschutzzentrum selbst angestellt sind. Es sind im Berichtszeitraum elf Stellen vorgesehen, die zum Jahresende auch alle besetzt sind.

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

	Soll	Ist
Diözesandatenschutzbeauftragter / Verbandsdatenschutzbeauftragter / Leiter KDSZ	1	1
Stellvertrentender Diözesandatenschutzbeauftragter / Stellvertretender Verbandsdatenschutzbeauftragter / Stellvertretender Leiter KDSZ	1	1
Referentinnen / Referenten	5	5
Sachbearbeiterinnen / Sachbearbeiter	2	2
Sekretariat	2	1,77
Gesamt	11	10,77

Personalausstattung KDSZ zum 31.12.2019 (in Vollzeitstellen)

Bei der Planung des Katholischen Datenschutzzentrums wurde konsequent auf die Umsetzung des Urteils des Europäischen Gerichtshofs vom 09.03.2010 zur Unabhängigkeit und Selbständigkeit der Datenschutzaufsichtsbehörden[17] geachtet und die Veränderungen durch die Europäische Datenschutz-Grundverordnung beziehungsweise deren Umsetzung in kirchliches Recht schon berücksichtigt.

Das Katholische Datenschutzzentrum hat seinen Sitz in der Kommende Dortmund, dem Standort des Sozialinstituts der Erzdiözese Paderborn.

Nach der Übernahme der Aufgaben des Diözesandatenschutzbeauftragten der fünf (Erz-)Diözesen in NRW zum 01.09.2016, dem Aufbau der Einrichtung im Jahr 2017 und der Beratung zu den alten und neuen Anforderungen des Kirchlichen Datenschutzgesetzes im Jahr 2018, konnte im Berichtszeitraum das umfangreiche Beratungsangebot für die kirchlichen Einrichtungen trotz der hohen Arbeitsbelastung mit

17 Siehe hierzu auch Abschnitt 5.1.1 dieses Jahresberichts.

Beschwerden und gemeldeten Datenschutzverletzungen weiter sichergestellt werden.

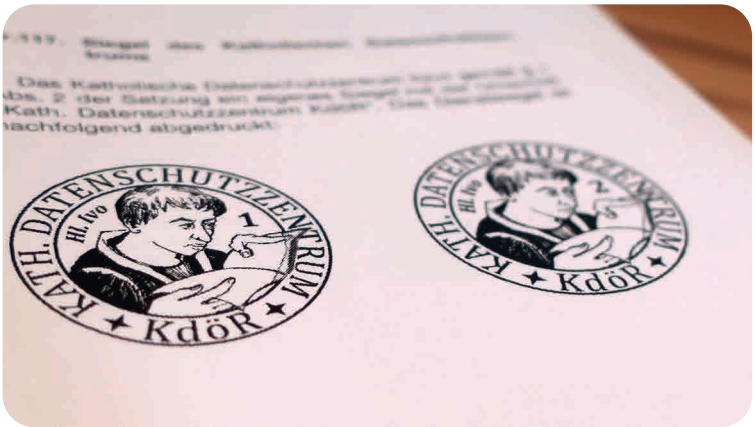
Mit der Übernahme der Datenschutzaufsicht über den VDD und die angeschlossenen Einrichtungen wurde diese Aufgabe in die bestehenden Abläufe des Katholischen Datenschutzzentrums integriert und so die reibungslose Wahrnehmung der Datenschutzaufsicht auch für diese kirchlichen Stellen sichergestellt.

4.3 Der hl. Ivo – Schutzpatron des Katholischen Datenschutzzentrums

Mit der Gründung des Katholischen Datenschutzzentrums als der gemeinsamen Datenschutzaufsicht der fünf nordrhein-westfälischen (Erz-)Diözesen wurde dem Katholischen Datenschutzzentrum von den (Erz-)Diözesen auch ein Schutzpatron mitgegeben.

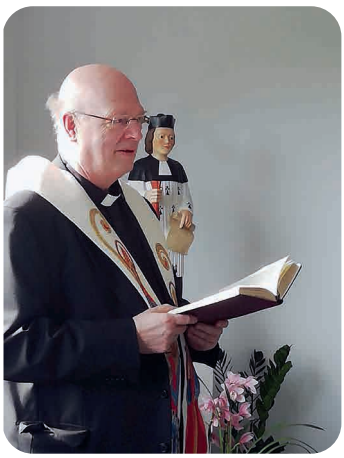
Der hl. Ivo lebte im 13. Jahrhundert in der Bretagne. Der Bischof von Tréguier ernannte den Priester, der auch Rechtswissenschaften studiert hatte, zu seinem Offizial. Dieses kirchliche Richteramt füllte er mit Mut und Unbestechlichkeit aus und setzte sich vor allem für Arme und Bedrängte vor weltlichen und kirchlichen Gerichten ein, was ihm den Ruf eines „Anwalts der Armen" einbrachte. Er wurde im 14. Jahrhundert heiliggesprochen. Sein Gedenktag ist der 19. Mai. Die Reliquien des heiligen Ivo werden in der Kathedrale von Tréguier aufbewahrt[18].

Das Bildnis des hl. Ivo ziert auch das Siegel des Katholischen Datenschutzzentrums, so dass der Schutzpatron auch in der täglichen Arbeit immer gegenwärtig ist.



Siegel des Katholischen Datenschutzzentrums, veröffentlicht im Amtsblatt der Erzdiözese Paderborn. (Bild: KDSZ)

18 Ausführlich zum Leben und Wirken des hl. Ivo: Michael Streck / Annette Rieck, St. Ivo (1247-1303) - Schutzpatron der Richter und Anwälte, 2007; Artikel „Ivo Hélory" auf Wikipedia (https://de.wikipedia.org/wiki/Ivo_Hélory). In dem Beitrag bei Wikipedia wird auch erwähnt, dass der hl. Ivo das Siegel des Katholischen Datenschutzzentrums ziert.



Generalvikar Alfons Hardt während der Segnung der Statue. (Bild: KDSZ)

Durch den persönlichen Einsatz des Generalvikars des Paderborner Erzbischofs und Vorsitzenden des Verwaltungsrates des Katholischen Datenschutzzentrums, Alfons Hardt, konnte das Katholische Datenschutzzentrum Anfang Mai 2019 eine Figur des hl. Ivo in seinen Räumen aufstellen und so die Verbindung zwischen dem Patron des Hauses und der Arbeit des Katholischen Datenschutzzentrums noch sichtbarer und erfahrbarer machen.

Am 13. Mai 2019 segnete Herr Generalvikar Hardt in Anwesenheit der Herren Generalvikare des Erzbistums Köln und der Bistümer Aachen, Essen und Münster sowie des Leiters des Katholischen Büros in Düsseldorf die Statue des hl. Ivo im Katholischen Datenschutzzentrum.

Von links nach rechts: Steffen Pau, Diözesandatenschutzbeauftragter und Leiter des Katholischen Datenschutzzentrums; Generalvikar Apostolischer Protonotar Alfons Hardt, Erzbistum Paderborn; Generalvikar Dr. Andreas Frick, Bistum Aachen; Generalvikar Dr. Klaus Winterkamp, Bistum Münster; Generalvikar Msgr. Dr. Markus Hofmann, Erzbistum Köln; Generalvikar Msgr. Klaus Pfeffer, Bistum Essen; Domkapitular Dr. Antonius Hamers, Leiter des Katholischen Büros NRW. (Bild: KDSZ)

4.4 Aufgabenkatalog

Die Aufgaben des Diözesandatenschutzbeauftragten beziehungsweise des Verbandsdatenschutzbeauftragten des VDDs als Datenschutzaufsicht sind im KDG beziehungsweise im KDG-VDD[19] 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 an die Datenschutzaufsicht wenden. Diese prüft den Sachverhalt und hört dazu die betroffene kirchliche Stelle an, soweit ein Verstoß gegen datenschutzrechtliche Regelungen vorliegen könnte. Wichtig ist dabei das Benachteiligungsverbot des § 48 Abs. 3 KDG: „Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an die Datenschutzaufsicht gewendet hat."

Das Überwachen 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 Grundlage von Informationen einer anderen Datenschutzaufsicht oder einer anderen Behörde."

Auf Basis dieser Regelung kann und muss die Datenschutzaufsicht Überprüfungen auf Grundlage der bei ihr eingehenden Beschwerden vornehmen. Sie kann aber auch ohne den konkreten Bezug zu einer Beschwerde anlasslos prüfen, ob die Einrichtungen das Gesetz richtig anwenden[20].

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, die Ermöglichung von Einsichtnahme in Akten und Räume zu unterstützen 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, aufgrund 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 werden, damit Datenschutz wirksam werden kann und die betroffenen Personen den gesetzlich vorgesehenen Schutz genießen können.

19 Im Folgenden wird nicht immer explizit auf die gleichlautende Vorschrift des KDG-VDD verwiesen.

20 Zur Auslegung der inhaltsgleichen Vorschrift des Art. 57 Abs. 1 lit. h) DSGVO vgl. Selmayr in Ehmann/Selmayr, Kommentar DSGVO, 2. Aufl. 2018, Art. 57 Rn. 9 und Kugelmann/Buchmann in Schwartmann u.a., Heidelberger Kommentar DSGVO / BDSG, 1. Aufl. 2018, Art. 57 Rn. 74.

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

4.5 Finanzen

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

Für das Kalenderjahr 2019 hat der Verwaltungsrat des Katholischen Datenschutzzentrums auf Vorschlag des Diözesandatenschutzbeauftragten den Haushaltsplan in Höhe von 1.400.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben bewilligt. Für das Folgejahr 2020 wird sich das genehmigte Budget leicht auf 1.375.000 Euro verringern.

4.6 Vertretung in Gremien und Arbeitsgruppen in der katholischen Kirche

Das Katholische Datenschutzzentrum bringt seine Kenntnisse und Erfahrungen aus der Praxis der Datenschutzaufsichten auch in die Arbeit von kirchlichen Gremien und Arbeitsgruppen ein. Die Beratung der Gremien und Arbeitsgruppen ist Teil des gesetzlichen Auftrags der Datenschutzaufsichten.

Im Berichtszeitraum unterstützte das Katholische Datenschutzzentrum die Arbeit mehrerer Unterarbeitsgruppen der Ständigen Arbeitsgruppe Datenschutz- und Melderecht / IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands durch Beteiligung an der Arbeit der Gremien. Diese Beteiligung erfolgte durch Stellungnahmen zu Gesetzentwürfen oder Einzelfragen, die im Rahmen dieser

kirchlichen Gesetzgebungsverfahren aufkamen. Teilweise nahm das Katholische Datenschutzzentrum an den Beratungen teil. Dabei kann die Datenschutzaufsicht ihre Expertise als unabhängiger Berater einbringen.

Als Datenschutzaufsicht für den VDD und die angeschlossenen Einrichtungen berät das Katholische Datenschutzzentrum darüber hinaus auch in datenschutzrechtlichen Fragen, die in anderen Gremien besprochen werden.

Bei der Weiterentwicklung der diözesanen Gesetze und der Diskussion von grundsätzlichen Rechtsfragen sind die 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.

4.7 Vernetzung

4.7.1 Vernetzung mit kirchlichen Stellen

Die fünf Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen stehen untereinander und mit den beiden gemeinsamen Ordensdatenschutzbeauftragten der Deutschen Ordensobernkonferenz in ständigem Austausch zu aktuellen Fragen und grundsätzlichen Themen. Die Besprechungen und Telefon- oder Videokonferenzen dienen diesem Austausch und der Vorbereitung und Verabschiedung gemeinsamer Beschlüsse[21].

Der Beauftragte für den Datenschutz der 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 es für kurze Vorträge und allgemeinen Erfahrungsaustausch zur Verfügung.

So hat das Katholische Datenschutzzentrum z.B. 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.

21 Siehe Abschnitt 5.1.2 dieses Jahresberichts zur Konferenz der Diözesandatenschutzbeauftragten und Abschnitt 5.2 zu den Beschlüssen der Konferenz.

4.7.2 Vernetzung mit staatlichen Stellen

Der Kontakt und der Austausch mit der Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten als staatlichen Datenschutzaufsichtsbehörden ist nach § 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 im kirchlichen Bereich bei Anwendung des KDG und im außerkirchlichen Bereich bei Anwendung der DSGVO sicherzustellen.

§ 18 Abs. 1 Satz 4 Bundesdatenschutzgesetz sieht eine Beteiligung der kirchlichen Datenschutzaufsichten bei bestimmten Sachverhalten vor, die vom Europäischen Datenschutzausschuss beraten werden, wenn die kirchlichen Datenschutzaufsichten von dieser 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. Die in der DSK zusammengeschlossenen unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder haben mit Beschluss vom 13.05.2019 („Beschluss zur Beteiligung der spezifischen Aufsichtsbehörden gem. § 18 Abs. 1 Satz 4 BDSG an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der EU“) ihren Standpunkt dazu festgehalten.[22]

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

4.8 Öffentlichkeitsarbeit

Das kirchliche Datenschutzrecht stellt ebenso wie die Datenschutz-Grundverordnung die Bedeutung der Information der Öffentlichkeit, der kirchlichen Stellen und der Verantwortlichen für die Datenverarbeitungen über Rechte und Pflichten beim Umgang mit personenbezogenen Daten besonders heraus. Der Aufgabenkatalog der Datenschutzaufsichten in § 44 Abs. 3 KDG betont dieses Thema gleich mehrfach.

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

22 Siehe Abschnitt 5.3.1 dieses Jahresberichts.

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).

Das Katholische Datenschutzzentrum macht daher 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.

4.8.1 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 und Vorlagen.

Teil der Internetseite des Katholischen Datenschutzzentrums ist auch ein gesichertes Kontaktformular. Über diese Kontaktmöglichkeit will das Katholische Datenschutzzentrum jedem Beteiligten eine gesicherte Kontaktaufnahme ermöglichen. Auf der Internetseite ist ebenfalls der öffentliche Schlüssel für die zentrale E-Mail-Adresse des Katholischen Datenschutzzentrums hinterlegt, so dass auch eine verschlüsselte Kommunikation per E-Mail möglich ist. Als weitere Möglichkeit der gesicherten Kommunikation hat das Katholische Datenschutzzentrum eine DE-Mail-Adresse eingerichtet.

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

4.8.2 Vorträge

Wie schon in den Vorjahren war auch im Berichtszeitraum die Nachfrage nach Vorträgen durch das Katholische Datenschutzzentrum hoch. Während im Jahr 2018 sehr stark Vorträge gefragt waren, die einen allgemeinen Überblick über die neuen, ab Mai 2018 geltenden gesetzlichen Regelungen geben sollten, gab es im Berichtszeitraum eine differenziertere Nachfrage. Neben dem weiterhin aktuellen Thema der gesetzlichen Neuerungen im kirchlichen Datenschutzrecht kamen verstärkt zielgruppenspezifische Vorträge hinzu. Hierzu zählten sowohl Anfragen der Dienstgeberseite, wie auch von Seiten der Mitarbeitervertretungen, Anfragen betrieblicher Datenschutzbeauftragter oder von IT-Arbeitskreisen. Wie in den Vorjahren waren dabei verschiedenste Gruppen und

Formate vertreten. Bei diesen Informationsveranstaltungen ist das Katholische Datenschutzzentrum als Referent zugegen, organisiert die Veranstaltungen aber nicht selbst. Mit diesen Vorträgen konnten erneut hunderte Multiplikatoren und Verantwortliche erreicht werden.

Das Katholische Datenschutzzentrum stellt auf Basis der Anfragen einen weiterhin hohen Informationsbedarf der kirchlichen Stellen, der betroffenen Personen und der Öffentlichkeit zum kirchlichen Datenschutz fest.

4.8.3 Informationen/Broschüren/Arbeitshilfen/Muster

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

In diesen Publikationen behandelt das Katholische Datenschutzzentrum grundsätzliche oder aktuelle Themen, auf die es entweder selbst aufmerksam oder durch vermehrte Anfragen zu einem Thema ein erhöhter Informationsbedarf deutlich wird. Das Angebot an Informationen wurde auch im Berichtszeitraum weiter ausgebaut.

Ergänzt wird dies durch Gastbeiträge für Fachzeitschriften (z.B. „Kompakt" für Kindertageseinrichtungen der Caritas im Erzbistum Köln), mit denen allgemein oder auch sehr zielgruppenspezifisch über Datenschutzthemen informiert wird.

4.8.4 Symposium „Ein Jahr Gesetz über den Kirchlichen Datenschutz – Rückblick und Ausblick"

Mehr als 110 Teilnehmende aus den deutschen (Erz-)Diözesen trafen sich am 28. Mai 2019 auf Einladung des Katholischen Datenschutzzentrums in den Räumen des Katholisch-Sozialen Instituts des Erzbistums Köln in Siegburg zum Symposium „Ein Jahr Gesetz über den Kirchlichen Datenschutz (KDG) – Rückblick und Ausblick".

Bild: KDSZ / Nicole Cronauge

Nach einem Jahr seit Inkrafttreten des KDG nahm das Katholische Datenschutzzentrum diesen Zeitraum zum Anlass, das kirchliche Gesetz in einem Rückblick und einem Ausblick zu betrachten.

Zu Beginn der Veranstaltung berichtete Marcus Baumann-Gretza, Justitiar des Erzbistums Paderborn und Vorsitzender der Ständigen Arbeitsgruppe Datenschutz- und Melderecht/IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands, über die gesetzgeberischen Tätigkeiten der katholischen Kirche zum Datenschutz. Er betonte die Notwendigkeit eines eigenen kirchlichen Datenschutzes und erinnerte an die lange Tradition kirchlicher datenschutzrechtlicher Regelungen, die mit der ersten Anordnung über den kirchlichen Datenschutz bis in die siebziger Jahre zurückreicht.

Einen Blick auf die Situation im staatlichen Bereich warf Professor Dr. Dieter Kugelmann, der Vorsitzende der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder im Jahr 2019 und Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz, in seinem Beitrag zu den Erfahrungen mit einem Jahr Datenschutz-Grundverordnung. Dabei stellte er auch die vielfältigen Aufgaben der Datenschutzaufsichten unter der Geltung der DSGVO dar. Er wies darauf hin, dass auch die Datenschutzaufsichten in Bund und Ländern durch viele Beratungsanfragen und zu klärende Detailfragen an ihre Leistungsgrenzen gekommen wären.

Bild: KDSZ / Nicole Cronauge

Steffen Pau, Leiter des Katholischen Datenschutzzentrums, schloss sich dieser Beschreibung in seinem Rückblick auf ein Jahr kirchliches Datenschutzgesetz für die kirchlichen Aufsichten an. Er erinnerte daran, bei allen heute gebotenen Möglichkeiten der Datenverarbeitung den Grundrechtsschutz der Personen, deren Daten verarbeitet werden, nicht außer Acht zu lassen. Der Schutz der Daten sei möglich, ohne sämtliche Datenverarbeitungen einzustellen. Es gebe praxisgerechte Lösungen.

Im Rahmen der Neuordnung des kirchlichen Datenschutzrechts ist im letzten Jahr ein gerichtlicher Rechtsschutz auf dem Gebiet des Datenschutzes durch die Kirchliche Datenschutzgerichtsordnung eingerichtet worden. Hierüber sowie über die kirchlichen Gerichte in Datenschutzangelegenheiten referierte Professor Dr. Gernot Sydow. Er ist Professor

für Europäisches Verwaltungsrecht an der Universität Münster und Vorsitzender des Datenschutzgerichts der Deutschen Bischofskonferenz.

Mit dem Standard-Datenschutzmodell präsentierte der stellvertretende Landesbeauftragte für Datenschutz und Informationsfreiheit von Mecklenburg-Vorpommern, Gabriel Schulz, eine Möglichkeit zur Unterstützung der Umsetzung des kirchlichen Datenschutzes. Schulz betonte, ebenso wie Michael Tolk, Referent des Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland, bei seiner Vorstellung der IT-Sicherheitskonzepte in der Evangelischen Kirche, dass Datenschutz als ein dauerhafter Verbesserungsprozess gelebt werden müsse.

Dr. Rene Meis, technischer Referent bei der Landesbeauftragten für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen, erläuterte in seinem Vortrag den Begriff des Risikos als einen der zentralen Begriffe der neuen Gesetze. Auswahl und Bewertung der Maßnahmen zum Schutz der personenbezogenen Daten bei der Verarbeitung seien an dem Risiko zu orientieren, das dem Betroffenen durch die geplante Verarbeitung der Daten drohe, wobei auch fehlerhafte Verarbeitungen abseits der geplanten Verarbeitungen zu betrachten seien.

In ihrem abschließenden Vortrag warnte Katharina Nocun, Bürgerrechtlerin und Publizistin, eindringlich vor den Möglichkeiten der Profilbildung und der Datensammlung von Konzernen. Sie schilderte auf Basis eigener Erfahrungen, wie weit die Datensammlung im täglichen Leben bereits fortgeschritten sei.

„Aufgrund der positiven Rückmeldungen der Teilnehmenden … [ist] die nächste Veranstaltung … für Mai 2021 geplant."

Das Katholische Datenschutzzentrum kann ein positives Fazit zur Veranstaltung ziehen. Aufgrund der positiven Rückmeldungen der Teilnehmenden plant das Katholische Datenschutzzentrum, dieses Format in regelmäßigen Abständen durchzuführen und so den Dialog mit allen Beteiligten fortzusetzen, um gemeinsam auch zukünftig praxisgerechte Lösungen auftretender Fragen zum Datenschutz zu finden. Die nächste Veranstaltung ist für Mai 2021 geplant.

4.9 Erste Bußgelder in 2019

Das KDG sieht, anders als noch die frühere Anordnung über den kirchlichen Datenschutz, für die Diözesandatenschutzbeauftragten als Datenschutzaufsicht über die kirchlichen Stellen die Möglichkeit vor, bei Verstößen gegen das KDG eine Geldbuße zu verhängen. Diese kann im Einzelfall bis zu 500.000 Euro betragen.

Da in den ersten Monaten der Geltung des neuen Gesetzes erst einmal die Beratung und Hilfe bei der Umsetzung für die kirchlichen Stellen im Vordergrund stand und auch bei festgestellten Verstößen die Durchführung des eigentlichen Bußgeldverfahrens Zeit in Anspruch nimmt, verhängte das Katholische Datenschutzzentrum erst im zweiten Halbjahr 2019 erste Bußgelder.

Im letzten Quartal 2019 hat der Diözesandatenschutzbeauftragte nach Abschluss des jeweiligen Bußgeldverfahrens gegen drei kirchliche Einrichtungen Bußgelder erlassen.

Gemäß § 51 KDG kann die Datenschutzaufsicht eine Geldbuße gegen den Verantwortlichen oder Auftragsverarbeiter verhängen, wenn dieser vorsätzlich oder fahrlässig gegen Bestimmungen des KDG verstoßen hat. Bei der Möglichkeit der Verhängung einer Geldbuße handelt es sich um eine Ermessensvorschrift. Dies bedeutet, dass nicht jeder festgesellte Verstoß mit einer Geldbuße zu ahnden ist („Kann-Vorschrift"). Der Datenschutzaufsicht stehen mit den Maßnahmen aus § 47 Abs. 5 und 6 KDG verschieden kombinierbare Maßnahmen zur Verfügung. Die Geldbuße nach § 47 Abs. 6 KDG ist daher oft in ein Gesamtpaket von Maßnahmen eingebunden. Ziel ist es, das Datenschutzniveau in der jeweiligen Einrichtung dauerhaft zu erhöhen.

Bei der Bemessung der Höhe einer Geldbuße sind vor allem die in § 51 Abs. 3 KDG aufgeführten Kriterien zu berücksichtigen. Dabei gilt es, sowohl mildernde als auch schärfende Umstände zu berücksichtigen und in die Abwägung einzubeziehen.

Zwar erscheint die Geldbuße zunächst als die am stärksten eingreifende Maßnahme der Datenschutzaufsicht, jedoch ist die Ahndung eines datenschutzrechtlichen Verstoßes mittels einer Anordnung nach § 47 Abs. 5 KDG oftmals mit mehr Aufwand seitens des Verantwortlichen verbunden, als die Zahlung einer Geldbuße. Gerade die in § 47 Abs. 5 lit. c) KDG normierte Anordnungsmöglichkeit, die Datenverarbeitung einzustellen, dürfte in den meisten Einrichtungen zu größeren (auch finanziellen) Einbußen führen. Somit sollte stets berücksichtigt werden, dass die Datenschutzaufsichten nicht nur die Möglichkeit der Verhängung einer Geldbuße nutzen können, auch wenn dies in der Presse oftmals als besonders einschneidende Maßnahme dargestellt wird.

Trotz dessen zeigt schon die bisherige Zurückhaltung der kirchlichen Datenschutzaufsichten bei der Verhängung von Geldbußen, dass die Geldbuße als ultima ratio herangezogen wird.

Die Geldbußen in 2019 wurden in zwei Fällen für das unbefugte Offenlegen von Gesundheitsdaten im Sinne von § 4 Nr. 17 KDG als personenbezogene Daten der besonderen Kategorie gemäß § 4 Nr. 2 KDG verhängt. In einem weiteren Fall gab es eine Geldbuße wegen Nichtmeldung eines datenschutzrechtlichen Verstoßes nach § 33 KDG trotz Aufforderung zur Meldung durch die Datenschutzaufsicht. Gerade die gesetzlich normierten Pflichten des Verantwortlichen sollten daher besonders sorgfältig von den Einrichtungen beachtet werden, um Bußgelder an dieser Stelle zu vermeiden.

4.10 Gerichtsverfahren mit Beteiligung des Katholischen Datenschutzzentrums

Seit Inkrafttreten des Gesetzes über den Kirchlichen Datenschutz am 24. Mai 2018 hat jede betroffene Person neben der Beschwerde bei der Datenschutzaufsicht auch das Recht auf gerichtlichen Rechtsbehelf (vgl. § 49 KDG). Zuständiges Gericht für diese Antragsverfahren ist in erster Instanz das Interdiözesane Datenschutzgericht mit Sitz in Köln und in zweiter Instanz das Datenschutzgericht der Deutschen Bischofskonferenz mit Sitz in Bonn. Bislang sind zwei Entscheidungen der ersten Instanz veröffentlicht[23].

Das Katholische Datenschutzzentrum war im Berichtsjahr Beteiligter in zwei Antragsverfahren. In beiden Fällen richtete sich der Antrag der betroffenen Person gegen den jeweiligen Bescheid des Diözesandatenschutzbeauftragten, weil der Betroffene mit der Entscheidung der Datenschutzaufsicht nicht einverstanden war. Beide Entscheidungen des Interdiözesanen Datenschutzgerichts stehen noch aus.

4.11 Sprecher der Konferenz der Diözesandatenschutzbeauftragten

Die Diözesandatenschutzbeauftragten der katholischen Kirche treffen sich regelmäßig zu gemeinsamen Beratungen über aktuelle Themen und gemeinsame Anliegen aus dem Bereich des kirchlichen Datenschutzes. Sie unterstützen sich so gegenseitig in der Wahrnehmung ihrer Aufgaben und geben gemeinsame Empfehlungen heraus[24]. Diese Konferenz der DDSB wählt jährlich einen Sprecher. Für das Jahr 2019 war der Diözesandatenschutzbeauftragte der nordrhein-westfälischen (Erz-)Bistümer und Leiter des Katholischen Datenschutzzentrums Sprecher dieser Runde.

Mit dieser Funktion verbunden ist u.a. die Repräsentation der Konferenz in einigen Gremien, zu denen ein Vertreter der kirchlichen Datenschutzaufsichten eingeladen wird. So nimmt der Sprecher beratend an den Sitzungen des Gremiums teil, was auf Ebene des VDDs die Entwicklung des Datenschutzrechts in der katholischen Kirche begleitet. Außerdem nahm der Sprecher im Berichtszeitraum an zwei Treffen der staatlichen Datenschutzaufsichten mit den Datenschutzaufsichten im Bereich der Medien und der Kirche teil. Diese Treffen sind Teil des wichtigen und kontinuierlichen Austausches, den die Diözesandatenschutzbeauftragten mit den staatlichen Datenschutzaufsichten und den Datenschutzaufsichten der Medien führen.

23 Die Urteile sind abrufbar unter https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen/

24 Weitere Informationen zur Konferenz der Diözesandatenschutzbeauftragten finden Sie in Abschnitt 5.1.2 dieses Jahreserichts.

5 Dokumentation

5.1 Die Datenschutzaufsicht in der katholischen Kirche

5.1.1 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 aufgrund 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 DDSB nimmt die Funktion wahr, die im staatlichen Bereich der oder die Landesdatenschutzbeauftrage als Datenschutzaufsicht wahrnimmt.

Zur effektiven und effizienten Wahrnehmung der Aufgaben der Datenschutzaufsicht und in Umsetzung des Urteils des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsichtsbehörden aus dem Jahr 2010 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.

5.1.2 Konferenz der Diözesandatenschutzbeauftragten

Zu den Aufgaben des DDSB 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 DDSB 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, der Ständigen Arbeitsgruppe Datenschutz- und Melderecht / IT-Recht[25] 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 sechs Konferenzen der Diözesandatenschutzbeauftragten statt. Gegenstand der Beratungen waren sowohl aktuelle Fragestellungen als auch Grundsatzfragen zum KDG, die sich bei der Umsetzung der Anforderungen des Datenschutzrechts für die kirchlichen Einrichtungen ergeben haben. Die Beschlüsse der Sitzungen sind in diesem Bericht in Abschnitt 5.2 dokumentiert.

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

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

Die katholischen und evangelischen Datenschutzaufsichten haben vor dem Hintergrund vergleichbarer Anforderungen und Fragestellungen

25 Zukünftig: Unterkommission Datenschutz- und Melderecht / IT-Recht der Rechtskommission des VDD.

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 DDSB mit den Datenschutzaufsichten der Evangelischen Kirche in Deutschland zum 3. Ökumenischen Datenschutztag im April 2019 in Georgsmarienhütte.

5.1.3 FAQ zur Konferenz der Diözesandatenschutzbeauftragten

Zur Konferenz der DDSB werden immer wieder Fragen an uns herangetragen, die aus Sicht des Katholischen Datenschutzzentrums gerne beantwortet werden:

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 indirekt 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 aus Sicht des Katholischen Datenschutzzentrums daraus, dass es eine einheitliche Auslegung der Sachverhalte zwischen den Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen gibt. Für die kirchlichen Stellen bringen diese Beschlüsse aber daher 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[26].

Welche Funktion hat der Sprecher der Konferenz?

Die Konferenz wählt aus ihrer Mitte jährlich einen Sprecher. Seine Aufgabe ist die Vorbereitung und Leitung der Sitzungen der Konferenz. Außerdem nimmt er als Gast an der Ständigen Arbeitsgruppe Datenschutz- und Melderecht / IT-Recht[27] 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 unter ddsb@kdsz.de.

26 Siehe Beschluss „Rechtliche Qualität der Beschlüsse der Konferenz" vom 26.07.2018, abgedruckt in Abschnitt 6 des Jahresberichts 2018 des Katholischem Datenschutzzentrums.
27 Zukünftig: Unterkommission Datenschutz- und Melderecht / IT-Recht.

5.2 Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten im Jahr 2019

5.2.1 Verträge zur Auftragsverarbeitung mit externen Unternehmen

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 04. April 2019)

Die Konferenz der Diözesandatenschutzbeauftragten weist darauf hin, dass bei Abschluss von Verträgen kirchlicher Einrichtungen mit Stellen, die nicht dem KDG unterliegen, zumindest eine Bezugnahme auf das aktuelle KDG in den Vertragstext aufgenommen werden soll.

Erläuterung zu dem Beschluss

Soweit sich kirchliche Stellen bei der Verarbeitung personenbezogener Daten anderer Stellen bedienen, haben sie – je nach Gegenstand der Vereinbarung - ihre Pflichten nach dem KDG ertraglich abzusichern bzw. auch auf die andere Stelle zu übertragen. Dies wird regelmäßig durch die Bezugnahme auf das KDG im Vertrag geschehen.

Hat der Vertragspartner einen Vertrag, der ausreichende Regelungen zu Datenschutz enthält, aber auf die entsprechenden Normen der DSGVO verweist, sollte zumindest ein pauschaler Verweis auf das Kirchliche Datenschutzgesetz in den Vertrag aufgenommen werden.

Ist auch dieser pauschale Verweis nicht möglich, sollte in einem Begleitschreiben zum Vertrag auf das Kirchliche Datenschutzrecht (KDG) hingewiesen werden. Auch hier müssen aber ausreichende Regelungen zum Datenschutz im Vertrag vorhanden sein.

5.2.2 Umgang mit Bildern von Kindern und Jugendlichen

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 04. April 2019)

Mit Beschluss vom 4. April 2019 ist der Beschluss der Konferenz der Diözesandatenschutzkonferenz vom 18. April 2018 („Veröffentlichung von Fotos von Kindern und Jugendlichen unter 16 Jahren“) aufgehoben worden. Folgende Beschlüsse sollen den aufgehobenen Beschluss ersetzen:

1. Erhebung und Speicherung von Bildern

Für die Rechtmäßigkeit der Erhebung und Speicherung von Bildern von Kindern und Jugendlichen ist es nicht zwingend erforderlich, dass eine Einwilligung der Sorgeberechtigten vorliegen muss. Rechtsgrundlage für die Erhebung und Speicherung von Bildern kann auch - nach erfolgter Abwägung - das berechtigte Interesse nach § 6 Abs. 1 lit. g) KDG sein.

Grundsätzlich kann nicht ausgeschlossen werden, dass Bilder von Kindern und Jugendlichen auch im Rahmen des berechtigten Interesses nach § 6 Abs. 1 lit. g) KDG erhoben und gespeichert werden können.

Das berechtigte Interesse nach § 6 Abs. 1 lit. g) KDG erfordert in jedem Fall eine Interessenabwägung zwischen dem berechtigten Interesse des Verantwortlichen oder eines ritten an der Erhebung und Speicherung der Bilder und dem Interesse bzw. den Grundrechten und Grundfreiheiten der betroffenen Personen. Sofern das Interesse des Verantwortlichen oder des Dritten an der Erhebung und Speicherung der Bilder überwiegt, ist die Datenverarbeitung auch zulässig. Die Interessenabwägung ist vor der Erhebung und Speicherung von Bildern durchzuführen und unterliegt der vollständigen aufsichtsbehördlichen Kontrolle.

Da es sich um Bilder von Kindern und Jugendlichen handelt, sind deren Interessen besonderes zu werten und zu berücksichtigen. Relevant können hier insbesondere Merkmale wie z.B. das Alter des betroffenen Kindes, der Zweck der Verarbeitung oder die Gruppengröße, aber auch die Eingriffsintensität sowie die Wahrscheinlichkeit des Eintritts eines Schadens sein. Die durch den Verantwortlichen durchgeführte Interessenabwägung unter besonderer Berücksichtigung der Interessen der Minderjährigen ist auf Anforderung der Datenschutzaufsichtsbehörde nachzuweisen.

2. Verarbeitung durch Übermittlung/Verbreitung

Für den Fall, dass die Bilder durch eine Übermittlung/Verbreitung verarbeitet werden sollen, ist es in der Regel erforderlich, dass die Sorgeberechtigten einwilligen.

Ausnahmen können sich dann ergeben, wenn ein berechtigtes Interesse nach § 6 Abs. 1 lit. g) KDG vorliegt. Im Rahmen der durchzuführenden Interessenabwägung können die Grundsätze des § 23 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie herangezogen werden.

a) Einwilligung

Die Verarbeitung durch Übermittlung/Verbreitung von personenbezogenen Daten (hier konkret die Bilder von Kindern und Jugendlichen) ist in der Regel nur mit einer Einwilligung der Sorgeberechtigten zulässig. Die Verarbeitung durch Übermittlung/Verbreitung umfasst jeden Vorgang, durch den andere Personen, Stellen, Behörden oder Einrichtungen Kenntnis von den personenbezogenen Daten erlangen oder erlangen können. Konkret bedeutet dies, dass jede Herausgabe von personenbezogenen Daten aus der jeweiligen Einrichtung an bspw. Eltern, Presse, Internetseite, o.ä. eine Verarbeitung durch Übermittlung/Verbreitung darstellt.

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands sieht es als ausreichend an, wenn die Einwilligung für konkret benannte Veranstaltungen vor zw. bei Beginn des Schul- oder Kitajahres für das jeweilige Jahr eingeholt wird. Die Einwilligung kann entweder unmittelbar im Anmeldeprozess oder am ersten Schul- oder Kitatag eingeholt werden.

Das Erfordernis, dass das konkrete Bild im Zeitpunkt der Unterzeichnung der Einwilligungserklärung vorliegen soll, entfällt.

b) Berechtigtes Interesse

Ausnahmen zur Einwilligung können sich dann ergeben, wenn ein berechtigtes Interesse nach § 6 Abs. 1 lit. g) KDG vorliegt. Auch hier ist eine Interessenabwägung zwingend erforderlich s. Punkt 1). Insbesondere sind aufgrund der spezifischen Gefahren einer Verarbeitung durch Übermittlung/Verbreitung die Interessen der Kinder und Jugendlichen besonders zu berücksichtigen. Je größer der (un-)bekannte Personenkreis ist, der von den Bildern Kenntnis nimmt oder Kenntnis nehmen kann, desto höher und intensiver ist der Eingriff in die Interessen der die Grundrechte und Grundfreiheiten der Kinder und Jugendlichen. Im Rahmen der Interessenabwägung können die Grundsätze des § 23 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie herangezogen werden. Eine Dokumentation der durchgeführten Interessenabwägung ist auch auf Anforderung der Datenschutzaufsichtsbehörde nachzuweisen.

3. Grundsätzlicher Hinweis

Sofern der jeweilige Verantwortliche beabsichtigt, die Bilder aufgrund einer Einwilligung zu verarbeiten und die betroffene Person die Einwilligung nicht erklärt, nicht wirksam erklärt oder widerrufen hat, so ist ein Rückgriff auf das berechtigte Interesse oder eine andere Rechtsgrundlage ausgeschlossen.

4. Informations- und Transparenzpflichten

Sowohl bei der Erhebung und Speicherung als auch bei der Verarbeitung durch Übermittlung/Verbreitung von Bildern sind die Informationspflichten nach dem KDG einzuhalten. Während die Informationspflichten bei der Erhebung und Speicherung sowie bei der Verarbeitung durch Übermittlung/Verbreitung aufgrund einer Einwilligung keine Besonderheiten aufweisen, sind bei der Verarbeitung durch Übermittlung/Verbreitung aufgrund des berechtigten Interesses einige Punkte zu beachten. 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. Die insoweit vorhandene Informationspflicht kann aber nach § 15 Abs. 4 DG 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 § 15 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 die Teilnehmer ber die Anfertigung und die Verarbeitung durch Übermittlung/Verbreitung von Fotografien informiert. Ist eine solche Information aufgrund der Struktur der Veranstaltung von vorneherein unmöglich, spricht vieles dafür, dass die Erfüllung der Informationspflichten einen unverhältnismäßig großen Aufwand erfordern würde (vgl. § 15 Abs. 4 KDG).

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 ustehenden 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 demgegenüber eine überschaubare Menge von Personen fotografiert, ist der Verantwortliche natürlich verpflichtet, seinen Informationspflichten nach §§ 14-16 KDG nachzukommen.

Diese Bewertung des Umgangs insbesondere mit der Verarbeitung durch Übermittlung/Verbreitung von Fotos versteht sich als eine Erläuterung, welche ergänzt werden kann.

5.2.3 Muster zur Videoüberwachung

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 04. Juli 2019)

Die Konferenz der Diözesandatenschutzbeauftragten hat in Ihrer Sitzung am 04. Juli 2019 in Freising das beigefügte Muster inkl. Erläuterungen beschlossen.

Beispiel für ein vorgelagertes Hinweisschild nach § 15 KDG bei Videoüberwachung

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:
Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):
Zwecke und Rechtsgrundlage der Datenverarbeitung:
berechtigte Interessen, die verfolgt werden:
Speicherdauer oder Kriterien für die Festlegung der Dauer:

Ausfüllhinweise zum den Mustern "vorgelagertes Hinweisschild" und "Informationsblatt zur Videoüberwachung".

1. Informationsblatt zur Videoüberwachung

Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. § 14 KDG). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A3 erfolgen.

2. Vorgelagertes Hinweisschild

Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. § 14 KDG). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen. Die Hinweise zu den weiteren Informationen muss um die genaue Ortsangabe bzw. Fundstelle im Internet ergänzt werden.

3. QR-Code

Bei Verwendung des QR-Codes muss dieser durch einen von dem Verantwortlichen erstellten QR Code ersetzt werden. Bei dem im Muster abgebildeten QR Code handelt es sich um einen Platzhalter.

4. Name und Kontaktdaten des Verantwortlichen

Verantwortlich ist nach § 4 Nr. 9 KDG die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Falle von juristischen Personen (z.B. Gemeinden, GmbHs, Vereinen usw.) ist die Nennung des gesetzlichen Vertreters erforderlich.

5. Kontaktdaten des Datenschutzbeauftragten

Datenschutzbeauftragter ist der vom Verantwortlichen benannte Datenschutzbeauftragte. Hierbei kann es sich um einen betrieblichen Datenschutzbeauftragten oder um einen externen Datenschutzbeauftragten handeln.

6. Zwecke und Rechtsgrundlage der Datenverarbeitung

Die Erhebung von Daten per Videoüberwachung ist nur zulässig, wenn Sie die Voraussetzungen von §§ 6 ff KDG erfüllen. Die entsprechend zutreffende Rechtsgrundlage sowie der beabsichtigte Zweck müssen kurz in Schlagworten dargestellt werden.

7. Berechtigte Interessen

Die berechtigten Interessen des Verantwortlichen an der Durchführung der Videoüberwachung müssen kurz in Schlagworten dargestellt werden.

8. Speicherdauer, oder Kriterien für die Festlegung der Dauer

Bei einer festgelegten Speicherdauer muss die tatsächliche Speicherdauer, bei einer individuell bestimmten Speicherdauer, die Kriterien für die Festlegung der Speicherdauer angegeben werden.

9. Empfänger oder Kategorien von Empfängern der Daten

Empfänger ist nach § 4 Nr. 11 KDG eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt. Bitte geben Sie hier die Stellen der Empfänger an, die die entsprechenden Daten verarbeiten. Hierbei wird nicht nach der konkreten Person, sondern nach der verarbeitenden Stelle gefragt.

Beispiel für ein vollständiges Informationsblatt (Aushang) nach § 15 KDG bei Videoüberwachung

Sie finden diese Informationen zusätzlich im Internet unter …

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

Empfänger oder Kategorien von Empfänger der Daten (sofern Datenübermittlung stattfindet):

bei Absicht des Verantwortlichen, die personenbezogenen Daten **an ein Drittland oder eine internationale Organisation zu übermitteln:** Informationen über Angemessenheitsbeschluss der Kommission bzw. geeignete oder angemessene Garantien:

Hinweise auf die Rechte der Betroffenen

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf die in § 17 KDG im einzelnen aufgeführten Informationen.

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die **Berichtigung** sie betreffender unrichtiger personenbezogener Daten und ggf. die **Vervollständigung** unvollständiger personenbezogener Daten zu verlangen (§ 18 KDG).

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in § 19 KDG im einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (**Recht auf Löschung**).

Die betroffene Person hat das Recht, von dem Verantwortlichen die **Einschränkung der Verarbeitung** zu verlangen, wenn eine der in § 20 KDG aufgeführten Voraussetzungen gegeben ist, z. B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten **Widerspruch** einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (§ 23 KDG).

Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das **Recht auf Beschwerde bei der zuständigen Datenschutzaufsicht**, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Regelungen des KDG verstößt (§ 48 KDG). Die betroffene Person kann dieses Recht bei der zuständigen Datenschutzaufsicht geltend machen. In der Diözese (Name Diözese) ist die zuständige Datenschutzaufsicht: …

5.2.4 Zur Einwilligung bei schlechteren technischen und organisatorischen Maßnahmen

(Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 19. September 2019)

In der Praxis kommt es zu Fällen, in denen die betroffene Person eine Einwilligung in Abweichungen von Aspekten der Datensicherheit erteilen soll. Beispielhaft zu nennen ist an dieser Stelle die Einwilligung in unverschlüsselte Kommunikation per Email beim Versand von besonderen Kategorien personenbezogener Daten.

Da in diesen Fällen regelmäßig die Einwilligung nach § 6 Absatz 1 lit b) bzw. § 11 Absatz 2 lit a) KDG nicht als eigentliche Rechtsgrundlage für die Verarbeitung dienen soll, sondern hier für eine an sich schon gerechtfertigte Verarbeitung eine negative Abweichung von technischen Schutzmaßnahmen zum Datenschutz legitimiert werden soll, kann die Einwilligung diese Abweichung des durch § 26 KDG gesetzlich geforderten Schutzstandards nicht erreichen.

Die Konferenz der Diözesandatenschutzbeauftragten hat daher folgenden Beschluss gefasst:

Die Konferenz der Diözesandatenschutzbeauftragten beschließt für sich folgende Auslegung des KDG in dieser Frage:

1. Die in § 26 KDG normierte Verpflichtung des Verantwortlichen, geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus zu treffen, ist zwingender Natur und steht mithin nicht zur Disposition der an der Datenverarbeitung Beteiligten.
2. Insbesondere darf eine Einwilligung im Sinne des § 6 Absatz 1 lit. b) bzw. § 11 Absatz 2 lit. a) KDG nicht verlangt werden, um nicht ausreichend geeignete technische und organisatorische Maßnahmen durch den Betroffenen zu legitimieren.

5.3 Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder (DSK) - Auszug -

5.3.1 Beschluss vom 13. Mai 2019

(Beschluss zur Beteiligung der spezifischen Aufsichtsbehörden gem. § 18 Abs. 1 Satz 4 BDSG an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der EU)

1. Die Verpflichtung zur Beteiligung der spezifischen Aufsichtsbehörden nach § 18 Abs. 1 Satz 4 BDSG ist nur dann eröffnet, wenn es sich um Angelegenheiten der Europäischen Union handelt.

2. Liegen die Voraussetzung von Nr. 1 vor, ist eine Betroffenheit in folgenden Konstellationen gegeben:

a) eine spezifische Aufsichtsbehörde ist im Kooperationsverfahren nach Art. 60 DSGVO unmittelbar selbst federführende Behörde im Sinne von § 19 Abs. 1 BDSG (vgl. Art. 56 DSGVO);

b) eine spezifische Aufsichtsbehörde ist für die Bearbeitung einer Eingabe entsprechend § 19 Abs. 2 BDSG (vgl. Art. 4 Nr. 22 Buchst. c DSGVO) zuständig;

c) eine spezifische Aufsichtsbehörde ist in entsprechender Anwendung von § 40 Abs. 2 BDSG n der Rolle als betroffene Behörde (vgl. Art. 4 Nr. 22 Buchs. a DSDGVO) zuständig;

d) eine spezifische Aufsichtsbehörde ist in den Verfahren nach Art. 60 DSGVO in der Konstellation des Art. 4 Nr. 22 Buchst. b DSGVO betroffen, wenn sich die erheblichen Auswirkungen nur im Rahmen der ausschließlichen Zuständigkeiten der spezifischen Aufsichtsbehörde bewegen;

e) ein Verfahren der Amtshilfe nach Art. 61 DSGVO oder gemeinsame Maßnahmen spielen sich unmittelbar im Zuständigkeitsbereich einer spezifischen Aufsichtsbehörde ab.

3.

a) Im Kohärenzverfahren nach Art. 64 DSGVO, ggf. zusätzlich im Verfahren der verbindlichen Streitbeilegung nach Art. 65 DSGVO (bei unmittelbarer Zuständigkeit siehe oben 2); und

b) bei der Erarbeitung von Stellungnahmen und der Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren i. S. v. Art. 70 DSGVO liegt nur dann eine Betroffenheit vor, wenn spezifische Fragen der Verarbeitung personenbezogener Daten durch die der Aufsicht der spezifischen Aufsichtsbehörden unterliegenden Stellen betroffen sind.

Erläuterung: Spezifische Betroffenheit bedeutet, dass gerade die spezifische Aufsichtsbehörde in einer Weise von der Angelegenheit betroffen sein muss, die über ine allgemeine Mitbetroffenheit hinausgeht. Ist sie lediglich in gleicher Weise betroffen wie die staatlichen Aufsichtsbehörden, liegt keine spezifische Betroffenheit vor und die Beteiligungspflicht wird nicht ausgelöst. Dabei kommt es nicht nur darauf an, dass bspw. Kirchen, Religionsgemeinschaften oder Medien-/Rundfunkveranstalter ausdrücklich Gegenstand einer Angelegenheit sind. Eine spezifische Betroffenheit ist vielmehr auch dann anzunehmen, wenn der Gegenstand einer Angelegenheit in besonderer Weise den Zuständigkeitsbereich der spezifischen Aufsichtsbehörden berührt.

4. Die Aufsichtsbehörden des Bundes und der Länder können für alle weiteren Fälle eine Beteiligung vorsehen.

5. Die Verpflichtungen zur Beteiligung nach § 18 Abs. 1 Satz 4 BDSG sind erfüllt, wenn die spezifischen Aufsichtsbehörden frühzeitig mit allen zweckdienlichen Informationen versorgt sind und ihnen frühzeitig Gelegenheit zur Stellungnahme gegeben wird. Die Betroffenheit einer

spezifischen Aufsichtsbehörde wird von der Aufsichtsbehörde geprüft, die die Herstellung einer Positionsbestimmung in europäischen Angelegenheiten initiiert. Die Beteiligung der spezifischen Aufsichtsbehörden wird über die Zentrale Anlaufstelle sichergestellt. Die Aufsichtsbehörden des Bundes und der Länder berücksichtigen die Stellungnahmen der spezifischen Aufsichtsbehörden. Eine abweichende Stellungnahme ändert aber weder etwas an einem sonst unter den Aufsichtsbehörden von Bund und Ländern bestehenden Einvernehmen noch hat dies Auswirkungen auf Abstimmungen nach § 18 Abs. 2 BDSG.

6. Bei § 18 Abs. 1 Satz 4 BDSG handelt es sich um eine Verfahrensregelung, deren Nichteinhaltung keine rechtlichen Folgen für das Verfahren hat.

7. Die spezifischen Aufsichtsbehörden werden durch die Aufsichtsbehörden des Bundes und der Länder regelmäßig über die Entwicklungen auf europäischer Ebene informiert.

8. Gemeinsam mit dem BfDI lädt der Vorsitz der Datenschutzkonferenz Vertreter der spezifischen Aufsichtsbehörden zweimal jährlich zu einem Informations- und Erfahrungsaustausch ein.

9. Religions- und Weltanschauungsgemeinschaften können nach Artikel 91 Absatz 2 DSGVO nur dann eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, einrichten, wenn sie bereits zum Zeitpunkt des Inkrafttretens der DSGVO am 25. Mai 2016 umfassende Datenschutzregelungen i. S. v. Art. 91 Abs. 1 DSGVO angewendet haben. Diese Datenschutzregelungen müssen mit der DSGVO in Einklang gebracht werden.

10. Weitere Erläuterungen ergeben sich aus den Arbeitsergebnissen der 9. Sitzung des AK Grundsatz, die die DSK am 29. Januar 2019 zustimmend zur Kenntnis genommen hat.

5.3.2 Beschluss vom 12. August 2019

(Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu spezifischen Aufsichtsbehörden)

Nach der Sonderregelung des Artikel 91 Absatz 1 der Europäischen DatenschutzGrundverordnung (DSGVO) dürfen Kirchen, religiöse Vereinigungen oder Gemeinschaften, die zum Zeitpunkt des Inkrafttretens der DSGVO umfassende Regelungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten anwenden, diese weiter anwenden, sofern sie mit den Vorschriften der DSGVO in Einklang gebracht werden.

Grundsätzlich unterliegen auch die Kirchen, religiösen Gemeinschaften oder Vereinigungen, die bereits zum Zeitpunkt des Inkrafttretens der DSGVO am 25. Mai 2016 umfassende Datenschutzregelungen i. S. v. Artikel 91 Absatz 1 DSGVO angewendet haben, nach Artikel 91 Absatz 2 DSGVO der Aufsicht durch eine unabhängige Aufsichtsbehörde.

Artikel 91 Absatz 2 DSGVO erlaubt ihnen jedoch, eine unabhängige Aufsichtsbehörde spezifischer Art einzurichten.

Für Religionsgemeinschaften, die erst nach dem Inkrafttreten der DSGVO umfassende Datenschutzvorschriften erlassen (haben), ist der sachliche Anwendungsbereich der DSGVO uneingeschränkt eröffnet und es gilt die allgemeine Datenschutzaufsicht.

Bei Artikel 91 handelt es sich um eine Bestandsschutzregelung für die Datenschutzvorschriften derjenigen Kirchen und religiösen Vereinigungen oder Gemeinschaften, die zum Zeitpunkt des Inkrafttretens der DSGVO bereits ein umfassendes, in sich abgeschlossenes Datenschutzrecht etabliert hatten. Solche Religionsgemeinschaften sollen nicht gezwungen sein, ihr unter dem alten Recht bereits etabliertes Recht abschaffen zu müssen.

Die bestehenden Datenschutzregelungen müssen allerdings mit der DSGVO in Einklang gebracht worden sein. Dadurch soll trotz der Privilegierung dieser Regelungen ein einheitliches Niveau staatlichen und kirchlichen Datenschutzrechts erreicht werden.

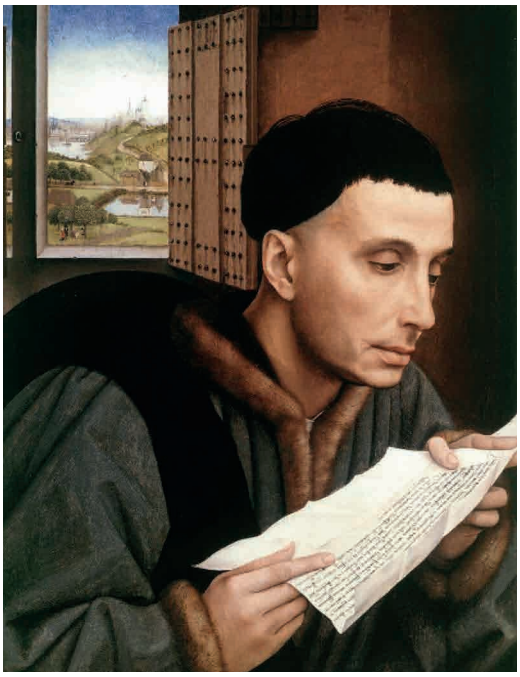
Die „spezifischen" Aufsichtsbehörden müssen darüber hinaus die in Kapitel VI der DSGVO für die unabhängigen Aufsichtsbehörden niedergelegten Voraussetzungen erfüllen. Das betrifft u.a. die Unabhängigkeit, Artikel 52 DSGVO, und die in Artikel 58 DSGVO geregelten Befugnisse.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sind gemäß § 18 Absatz 1 Satz 4 Bundesdatenschutzgesetz (BDSG) verpflichtet, diese spezifischen Aufsichtsbehörden bei der Zusammenarbeit in europäischen Angelegenheiten zu beteiligen, soweit sie betroffen sind.

Durch Anpassung des jeweils bereits vor dem 25. Mai 2016 bestehenden Gesetzes über den Kirchlichen Datenschutz sowie des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland an die DSGVO unterfallen zumindest die römisch-katholische Kirche bzw. die Adressaten des EKD-Datenschutzgesetzes grundsätzlich der durch Artikel 91 DSGVO ermöglichten Privilegierung.

Abkürzungsverzeichnis

BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BDSG a.F.	Bundesdatenschutzgesetz alter Fassung
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
CIC	Codex Iuris Canonici
DDSB	Diözesandatenschutzbeauftragte(r)
DOK	Deutsche Ordensobernkonferenz
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSGVO	Datenschutz-Grundverordnung (engl. GDBR)
DSK	Datenschutzklasse oder Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder
DVO	Durchführungsverordnung
EDPB	European Data Protection Board (dt. EDSA)
EDSA	Europäischer Datenschutzausschuss (engl. EDPB)
EKD	Evangelische Kirche in Deutschland
ENISA	Agentur der Europäischen Union für Cybersicherheit (engl. European Agency for Cybersecurity); Bezeichnung bis 28. Juni 2019: Agentur der Europäischen Union für Netz- und Informationssicherheit (engl. European Network and Information Security Agency)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GDPR	General Data Protection Regulation (dt. DSGVO)
GG	Grundgesetz
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GRCh	Charta der Grundrechte der Europäischen Union
IDSG	Interdiözesanes Datenschutzgericht
KDG	Gesetz über den Kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum KDG
KDM	Kirchliches Datenschutzmodell
KDO	Anordnung über den kirchlichen Datenschutz
KDSGO	Kirchliche Datenschutzgerichtsordnung
KDSZ	Katholisches Datenschutzzentrum
KIS	Krankenhausinformationssystem
OVG	Oberverwaltungsgericht
SDM	Standarddatenschutzmodell
VDD	Verband der Diözesen Deutschlands
§ 29-KDG-Gesetz	Gesetz zur Regelung des Rechtsinstruments nach § 29 Gesetz über den Kirchlichen Datenschutz



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.

Bild: 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