Jahresbericht 2017

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

Berichtszeitraum
01.01.–31.12.2017

Katholisches Datenschutzzentrum

Herausgegeben vom

Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn
sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil)

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

2. Jahresbericht

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

für den Zeitraum 01.01.2017 – 31.12.2017

Redaktionsschluss: 31. Juli 2018

Inhaltsverzeichnis

Inhaltsverzeichnis 4
Vorwort 6
1 Entwicklungen im Datenschutz 9
1.1 Entwicklungen in der Europäischen Union 9
1.1.1 Geltung der DSGVO ab 25. Mai 2018 9
1.1.2 Entwurf der ePrivacy-Verordnung 9
1.1.3 Entwicklungen zum Privacy Shield 9
1.1.4 Der Brexit und die Auswirkungen für den Datenschutz 11
1.2 Entwicklungen in der Bundesrepublik Deutschland 12
1.3 Entwicklungen in der römisch-katholischen Kirche 12
1.4 Entwicklungen in der evangelischen Kirche 14
1.5 Entwicklung in der Datensicherheit 14
1.5.1 BSI-Grundschutz überarbeitet 14
1.5.2 Standard-Datenschutzmodell 15
1.5.3 WLAN-Verschlüsselung nach WPA2-Standard 16
1.5.4 USB-Anschluss - praktisch, aber auch ein mögliches Sicherheitsrisiko 17
2 Die Datenschutzaufsicht in der katholischen Kirche 19
2.1 Struktur der Datenschutzaufsicht 19
2.2 Konferenz der Diözesandatenschutzbeauftragten 20
3 Aus der Tätigkeit des Datenschutzzentrums 23
3.1 Aufgabenkatalog (Beratung - Prüfung - Schulung) 23
3.2 (Vor-Ort-)Prüfungen und Prozessaufnahmen 25
3.3 Einzelne Themen beleuchtet 26
3.3.1 Auftrags(daten)verarbeitung 26
3.3.2 Videoüberwachung 28
3.3.3 Bring-Your-Own-Device (BYOD) 29
3.3.4 Unerlaubte Weitergabe von personenbezogenen Daten 31
3.3.5 Umgang mit Krankmeldungen im Arbeitsverhältnis 32

3.3.6 Cloud-Nutzung ... 32
3.3.7 Datenschutz in Pfarrgemeinden ... 33
3.3.8 Einwilligungen ... 34
3.3.9 Erweitertes Führungszeugnis ... 34
3.3.10 Messengerdienste ... 36
4 Vorbereitung auf das neue KDG ... 37
4.1 Benennung eines betrieblichen Datenschutzbeauftragten (bDSB) ... 37
4.2 Bestandsaufnahme der Verarbeitungsprozesse mit personenbezogenen Daten ... 38
4.3 Verträge und Dienstvereinbarungen überprüfen ... 39
4.4 Besonderen Schutz von Kindern und Jugendlichen sicherstellen ... 39
4.5 Betroffenenrechte umsetzen ... 39
4.6 Datenschutzkonzept erstellen oder vervollständigen ... 40
4.7 Verfahrensverzeichnis wird aufgewertet ... 41
4.8 Möglichkeit zur Vornahme einer Datenschutz-Folgenabschätzung einrichten ... 42
4.9 Haftung und Schadenersatz ... 43
5 Das Katholische Datenschutzzentrum ... 45
5.1 Zuständigkeitsbereich ... 45
5.2 Aufbau der Einrichtung ... 45
5.3 Finanzen ... 47
5.4 Vertretung in Gremien und Arbeitsgruppen in der katholischen Kirche ... 47
5.5 Vernetzung ... 48
5.5.1 Vernetzung mit kirchlichen Stellen ... 48
5.5.2 Vernetzung mit staatlichen Stellen ... 48
5.6 Öffentlichkeitsarbeit ... 49
6 Ausblick ... 51
7 Anhang - Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten im Jahr 2017 ... 53
7.1 Beschluss zur Nutzung von Messenger-Diensten ... 53
Abkürzungsverzeichnis ... 56

Vorwort

„2017 - das Jahr zwischen alt und neu“. So könnte eine Schlagzeile aus Sicht der Datenschützer für das Jahr 2017 lauten.

Mit der Verabschiedung der neuen Europäischen Datenschutzgrundverordnung (DSGVO) und dem Inkrafttreten Ende Mai 2016 begann die zweijährige Übergangszeit der DSGVO, die mit der Anwendbarkeit der neuen Regelungen am 25. Mai 2018 enden wird.

Das Jahr 2017 war bei den Einrichtungen im außerkirchlichen Bereich daher bestimmt durch Analysen der eigenen Datenverarbeitungen und eingesetzten Hard- und Software, der Ermittlungen der technisch-organisatorischen Schutzbedarfe und dem Abgleich mit den schon umgesetzten Schutzmaßnahmen. Benutzer- und Berechtigungskonzepte sowie bestehende Verträge über die Verarbeitung personenbezogener Daten wurden auf Änderungsbedarf überprüft.

Im November 2017 wurde von der Vollversammlung des Verbandes der Diözesen Deutschlands der Entwurf zur Neufassung des kirchlichen Datenschutzgesetzes verabschiedet. Inkrafttreten wird die neue Regelung am 24. Mai 2018.

"Der zu erwartenden Unsicherheit im Umgang mit den neuen Regelungen werden wir mit viel Beratungseinsatz und Informationen in vielfältiger Weise zu begegnen versuchen."

Damit begann für die kirchlichen Einrichtungen die Übergangszeit zur Umsetzung der neuen Regelungen, die kürzer ausfiel, als die Frist für Unternehmen zur Umsetzung der DSGVO. Auf Grund der Vorgaben zur Umsetzung der DSGVO war hier für den kirchlichen Gesetzgeber keine längere Frist möglich.

Vor dem Hintergrund der neuen Regelungen, der schon seit Jahren zunehmenden Sensibilität der Betroffenen über den Umgang mit ihren personenbezogenen Daten und den mit dem neuen Gesetz kommenden weitergehenden Befugnissen der Datenschutzaufsichten schauen sich viele kirchliche Einrichtungen ihre Verarbeitungen personenbezogener Daten nochmals – leider in Einzelfällen auch erstmals - genauer an, um die Verarbeitungen an die neuen Regelungen anzupassen.

Wenn auch der Arbeitsaufwand derzeit etwas größer erscheint - teilweise auch durch Nachholbedarf bei der Umsetzung schon bestehender Regelungen - wird der Schutz personenbezogener Daten der Betroffenen durch die neuen Regelungen gestärkt.

Der zu erwartenden Unsicherheit im Umgang mit den neuen Regelungen werden wir mit viel Beratungseinsatz und Informationen in vielfältiger Weise zu begegnen versuchen.

Der Auf- und Ausbau des Katholischen Datenschutzzentrums konnte im Berichtsjahr 2017 wie geplant fortgesetzt werden. Die Arbeitsfähigkeit wurde sowohl im personellen Bereich wie auch im Bereich der Arbeitsmittel weiter verbessert.

Zum 01.01.2018 übernimmt das Katholische Datenschutzzentrum auch die Datenschutzaufsicht für den Verband der Diözesen Deutschlands (VDD) als Rechtsträger der Deutschen Bischofskonferenz mit den angeschlossenen Einrichtungen.

Mit dieser Erweiterung der Zuständigkeit kann das Katholische Datenschutzzentrum seinen erfolgreichen Weg der ersten Monate der Tätigkeit fortsetzen.

Steffen Pau
Diözesandatenschutzbeauftragter
und Leiter des Katholischen Datenschutzzentrums

1 Entwicklungen im Datenschutz

1.1 Entwicklungen in der Europäischen Union

Auch wenn mit der DSGVO die große Datenschutzreform im Jahr 2016 verabschiedet worden ist, so gab es auch im Jahr 2017 auf europäischer Ebene wichtige Entwicklungen für den Datenschutz.

1.1.1 Geltung der DSGVO ab 25. Mai 2018

Die Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, besser bekannt als Europäische Datenschutz-Grundverordnung (DSGVO), die am 24. Mai 2016 in Kraft getreten ist, wird ab dem 25. Mai 2018 ihre endgültige Geltung erfahren und damit die europaweite Rechtsgrundlage in den Ländern der Europäischen Union darstellen. Inhaltliche Änderungen am Verordnungstext gab es im Berichtszeitraum nicht. Die Arbeit auf europäischer Ebene verlagerte sich in die Art. 29-Gruppe, wo die Datenschutzaufsichten die neuen Regelungen mit ihren Stellungnahmen und Working Papers operationalisieren.

1.1.2 Entwurf der E-Privacy Verordnung

Derzeit wird auf europäischer Ebene der Entwurf der ePrivacy-Verordnung beraten. Der Entwurf der „Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)“ soll die bestehende ePrivacy-Richtlinie der EU ersetzen, die in Deutschland schwerpunktmäßig in dem Telekommunikationsgesetz (TKG) und Telemediengesetz (TMG) umgesetzt wurde.

Diese Verordnung hat vor allem die elektronische Kommunikation im Blickfeld und wird für dieses Gebiet auch Änderungen in datenschutzrechtlicher Hinsicht mit sich bringen. Die abschließenden Verhandlungen zum Inhalt der Verordnung auf europäischer Ebene stehen noch aus. Die konkreten Auswirkungen der neuen Verordnung können daher erst zu einem späteren Zeitpunkt bewertet werden.

1.1.3 Entwicklungen zum Privacy Shield

Das Datenschutzrecht setzt nicht nur eine Rechtsgrundlage für jede Verarbeitung personenbezogener Daten voraus. Bei Verarbeitungen, die einen Drittlandsbezug haben, also eine Datenverarbeitung außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschafts-

raumes (EWR) vorsehen, ist neben der Rechtsgrundlage auch noch die Prüfung eines angemessenen Schutzniveaus für die Daten erforderlich.

"Der Mechanismus des Privacy Shields wird regelmässig jährlich durch die Europäische Kommision überprüft ..."

Dies bedeutet, dass geeignete Rechtsgrundlagen bereitstehen und hinreichende Vorkehrungen getroffen sind, um einen gesicherten Datenaustausch zu gewährleisten. Für den Bereich der EU bzw. des EWR wird dies durch die DSGVO gewährleistet. Für den Datentransfer in bzw. aus Ländern außerhalb dieses Bereichs, sog. Drittländer, bedarf es weiterer Instrumentarien, um die Zulässigkeit zu begründen. Die Vorgaben für eine zulässige Übermittlung personenbezogener Daten in Drittländer enthält Kapitel V der DSGVO. Dazu gehört auch das Instrument des Angemessenheitsbeschlusses durch die Europäische Kommission. Im Verhältnis zu den USA ist derzeit der Mechanismus des „Privacy Shield" die einschlägige Regelung. Dieser ist entwickelt worden, nachdem der Europäische Gerichtshof (EuGH) gefordert hatte, die Vorgängerregelung „Safe Harbor" zu beenden. Der Mechanismus des Privacy Shield wird regelmäßig jährlich durch die Europäische Kommission überprüft, zuletzt im September 2017. Die regelmäßige gemeinsame Überprüfung durch die Europäische Kommission und die US-Regierung ist in den Vereinbarungen zum Privacy Shield festgelegt. Der Privacy Shield ist - als Spezialfall der Angemessenheitsentscheidung - insoweit von Bedeutung, als er die Grundlage für Datentransfers in die USA darstellen kann, soweit das amerikanische Unternehmen dem Privacy Shield beigetreten ist und die Anforderungen erfüllt.

Nunmehr haben die an der Art. 29-Gruppe beteiligten europäischen Datenschutzbehörden Kritik an der derzeitigen Fassung des Privacy Shield geäußert und für die Übermittlung von personenbezogenen Daten in die USA von der Europäischen Kommission Nachbesserungen gefordert. Die Art. 29-Gruppe hat insbesondere angezweifelt, dass das Datenschutzniveau in den USA tatsächlich gleichwertig zu dem Datenschutzniveau in der Europäischen Union ist, insbesondere im Hinblick auf die neuen Regelungen der DSGVO. Die Entwicklung in diesem Prozess ist zu beobachten, da sie möglicherweise dazu führen kann, dass der Privacy Shield ähnlich wie die Regelung Safe Harbor als nicht ausreichende Rechtsgrundlage angesehen wird. Dies hätte möglicherweise eine Aufhebung zur Folge, wodurch ein Datenaustausch – sofern nicht eine geeignete Nachfolgeregelung rechtzeitig bereitsteht – in die USA nicht mehr zulässig wäre, zumindest nicht sofern nicht weitere Voraussetzungen nach der DSGVO durch Einzelregelungen oder Entscheidungen von Datenschutzaufsichtsbehörden für einen akzeptablen Datenaustausch geschaffen werden.

Auch wenn die Europäische Kommission den Privacy Shield nach der Überprüfung bestätigt hat, so ist vor dem Europäischen Gerichtshof mittlerweile ein Verfahren zur Vereinbarkeit des Privacy Shield mit europarechtlichen Vorgaben anhängig. Hier sollte die Entwicklung genau beobachtet werden.

Das Stichwort: Art. 29-Gruppe
Die Art. 29-Gruppe ist derzeit das maßgebende Gremium für die Zusammenarbeit der Mitgliedstaaten der Europäischen Union auf dem Gebiet des Datenschutzes. Sie ist noch nach den Vorgaben der Datenschutzrichtlinie 95/46/EG gebildet. Diese Richtlinie stellt die Grundlage für das bisherige Bundesdatenschutzgesetz dar. Aufgabe der Art. 29-Gruppe ist es, dass sich die Datenschutzaufsichtsbehörden aller Mitgliedstaaten der Europäischen Union untereinander abstimmen und die Europäische Kommission beraten können. Mit der Geltung der DSGVO ab dem 25. Mai 2018 wird dieses Gremium durch den Europäischen Datenschutzausschuss (EDSA) abgelöst. Dieser ist eine Einrichtung der Europäischen Union mit eigener Rechtspersönlichkeit und nimmt seine Aufgaben und Befugnisse weisungsunabhängig war. Seine Kernaufgabe ist es, die einheitliche Anwendung der DSGVO innerhalb der EU sicherzustellen. Dem EDSA steht eine beratende Funktion im Blick auf datenschutzrechtliche Fragestellungen auf europäischer Ebene zu, insbesondere auch zu Gesetzesvorschlägen der Europäischen Kommission. Der EDSA besteht aus Leiterinnen und Leitern der Datenschutzaufsichtsbehörden der europäischen Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten. Die Bundesrepublik Deutschland ist durch die Bundesdatenschutzbeauftragte im EDSA vertreten. Diese hat eine Stellvertretung, die aus dem Kreis der Leiterinnen und Leiter der Datenschutzaufsichtsbehörden der Bundesländer durch den Bundesrat gewählt wird.

1.1.4 Der Brexit und die Auswirkungen für den Datenschutz

Nachdem die Bürger in Großbritannien Mitte 2016 für ein Ausscheiden des Landes aus der Europäischen Union gestimmt hatten, hat die britische Regierung Ende März 2017 den Austritt aus der EU erklärt und damit die 24-monatige Übergangsphase gestartet. Der Austritt wird dann Ende März 2019 wirksam.

Sollte es in der Übergangsphase zu keinen vertraglichen Vereinbarungen zwischen der EU und Großbritannien zur zukünftigen politischen und wirtschaftlichen Zusammenarbeit kommen, droht ein ungeregelter Austritt Großbritanniens aus der EU. In diesem Fall würden die EU-Vorgaben nach dem Austritt in Großbritannien nicht mehr gelten und somit auch die DSGVO nicht mehr anwendbar sein.

Hier wird abzuwarten sein, welche Vereinbarungen bezüglich eines zulässigen Datenaustausch zwischen den übrigen Staaten der Europäischen Union und Großbritannien getroffen werden. Bei einem Austritt aus der Europäischen Union wäre Großbritannien nicht mehr Teil der durch die Zugehörigkeit zu diesem Staatenbund bezüglich eines Datenaustauschs privilegierten Staaten. Nach derzeitigem Beratungsstand würde Großbritannien auch nicht mehr zum Europäischen Wirtschaftsraum gehören mit der Folge, dass Großbritannien auf den Status eines

„Drittlandes“ im Sinne der DSGVO zurückgeworfen würde und zukünftig die Frage der Beurteilung des ausreichenden Datenschutzniveaus in Großbritannien zu klären sein würde. Auch muss beobachtet werden, welche gesetzlichen Grundlagen der britische Gesetzgeber im Bereich des Datenschutzes entwickeln und wie die Europäische Kommission diese dann beurteilen wird. Die Entwicklung hat Auswirkung auf Kooperationen mit britischen Firmen sowie auf die Nutzung von Programmen und Angeboten aus Großbritannien.

1.2 Entwicklungen in der Bundesrepublik Deutschland

Mit Art. 1 des Datenschutz-Anpassungs- und –Umsetzungsgesetzes EU – DSAnpUG-EU – vom 30. Juni 2017 ist für den Bereich der Bundesrepublik Deutschland das neue Bundesdatenschutzgesetz (BDSG) verabschiedet worden, welches parallel zur DSGVO am 25. Mai 2018 in Kraft treten wird. Es dient der Umsetzung der DSGVO und der Ausfüllung der den nationalen Gesetzgebern in der DSGVO gewährten Ermächtigungsgrundlagen zur Schaffung besonderer nationaler Regelungen. Das BDSG gilt für den dort bezeichneten Zuständigkeitsbereich und ist, von den diesem Gesetz unterfallenden Stellen, neben der DSGVO zu beachten.

Das neue BDSG enthält mit § 18 Abs. 1 Satz 4 eine auch für die kirchlichen Datenschutzaufsichten wichtige Regelung. Dort heißt es zur Beteiligung der kirchlichen Aufsichten bei der Abstimmung gemeinsamer Standpunkte: „Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach den Artikeln 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.“ Damit können die Interessen des kirchlichen Datenschutzes auch bei der Auslegung des neuen Datenschutzrechts auf europäischer Ebene eingebracht werden.

In den Bundesländern werden derzeit die landesrechtlichen Bestimmungen auf die Notwendigkeit der Anpassung der landesrechtlichen Regelungen, insbesondere der Landesdatenschutzgesetze, hin überprüft.

1.3 Entwicklungen in der römisch-katholischen Kirche

Auf der Vollversammlung des Verbandes der Diözesen Deutschlands (VDD) haben die (Erz-)Bischöfe am 20. November 2017 die Musterfassung des Gesetzes über den Kirchlichen Datenschutz (KDG) einstimmig beschlossen und den (Erz-)Diözesen in Deutschland zur Inkraftsetzung und Veröffentlichung empfohlen. Diese Musterfassung wurde von den (Erz-)Diözesen in ein diözesanes Gesetz umgesetzt,

vom jeweiligen Diözesanbischof unterzeichnet und in den kirchlichen Amtsblättern veröffentlicht.[1]

Ergänzt wird das neue KDG von einem weiteren Gesetz, das erstmals einen Rechtsweg für Datenschutzfragen vorsieht. Mit dieser Gerichtsordnung wird den Anforderungen der DSGVO entsprochen, die sowohl für die betroffenen Personen als auch für die Einrichtungen als Verantwortlichen Rechtsschutzmöglichkeiten gegen die Entscheidungen der Datenschutzaufsicht vorsehen. Das Gesetz wird eigene Spruchkörper für den Datenschutz vorsehen.

"Ergänzt wird das neue KDG von einem weiteren Gesetz, das erstmals einen Rechtsweg für Datenschutzfragen vorsieht."

Die Katholische Kirche hat damit die Anforderungen des Art. 91 DSGVO erfüllt. Die bei Inkrafttreten der DSGVO im Mai 2016 bestehende Anordnung über den kirchlichen Datenschutz (KDO) wurde vor Anwendbarkeit der DSGVO am 25. Mai 2018 mit den Regelungen der DSGVO in Einklang gebracht. Außerdem besteht mit dem Katholischen Datenschutzzentrum eine unabhängige Aufsicht im Sinne des Art. 91 Abs. 2 DSGVO für die nordrhein-westfälischen (Erz-)Diözesen.

Im Zuge der Schaffung eines neuen Rechts und der Ablösung der bisherigen Anordnungen über den kirchlichen Datenschutz (KDO) sind auch die weiteren Rechtsgrundlagen der (Erz-)Diözesen in Deutschland auf ihre Konformität mit den Grundvorgaben des KDG zu überprüfen. Dazu gehört insbesondere die bisherige Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO). Ebenso zählen dazu die als Gesetze erlassenen Grundlagen, z. B. die Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche (Kirchliche Archivordnung – KAO) oder die Anordnung über das kirchliche Meldewesen (Kirchenmeldewesenanordnung – KMAO) sowie die in einigen (Erz-)Diözesen erlassene Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen. Darüber hinaus sind die als Verwaltungsakte des Generalvikars auf der Grundlage des bisherigen § 22 KDO erlassenen Ausführungsbestimmungen, z. B. die Ausführungsrichtlinien zur Anordnung über den kirchlichen Datenschutz – KDO – für den pfarramtlichen Bereich, auf Konformität mit dem KDG zu prüfen. Für die Weitergeltung der übrigen bischöflichen Gesetze mit datenschutzrechtlichem Bezug sind in § 58 KDG Regelungen getroffen worden. Bezüglich der Ausführungsbestimmungen nach § 22 KDO sind in § 57 Absatz 5 KDG Übergangsbestimmungen für die Fortgeltung und deren verbleibende Dauer bis zur Außerkraftsetzung festgelegt.

1 Amtsblatt des Erzbistums Köln 2018, Nr. 12, S. 13 ff.; Kirchliches Amtsblatt für die Erzdiözese Paderborn 2018, Nr. 23 (S. 48 ff.); Kirchlicher Anzeiger für die Diözese Aachen vom 01.03.2018, Nr. 32, S. 78 ff.; Kirchliches Amtsblatt Bistum Essen 2018, Nr. 3 (S. 33 ff.); Kirchliches Amtsblatt für die Diözese Münster 2018, Art. 45 (S. 56 ff.).

1.4 Entwicklungen in der evangelischen Kirche

Die Evangelische Kirche Deutschlands (EKD) hat mit dem EKD-Datenschutzgesetz (DSG-EKD) ebenso wie die Katholische Kirche mit der KDO bereits seit Jahren eigene Regelungen zum Datenschutz in Kraft.
Dieses Gesetz ist ebenso überarbeitet worden die KDO. Mit der Überarbeitung hat die EKD ihr Datenschutzrecht ebenfalls den Erfordernissen des Art. 91 DSGVO entsprechend mit der DSGVO in Einklang gebracht.

1.5 Entwicklung in der Datensicherheit

Im Bereich des technisch-organisatorischen Datenschutzes gab es im Jahr 2017 mit der Überarbeitung des BSI-Grundschutzes und der weiteren Konzeptionierung des Standard-Datenschutz-Modells zwei nennenswerte Änderungen. Daneben haben viele Angriffe auf die eingesetzten Hard- und Softwaresysteme und neue bekanntgewordene Lücken in Hard- und Software gezeigt, dass immer neue Angriffsszenarien auf die IT der kirchlichen Einrichtungen ausprobiert werden und dass die eingesetzte Hard- und Software nicht immer frei von Mängeln ist und daher regelmäßig Updates erhalten sollte.

Viele neue Sicherheitstechniken machen IT-Systeme sicherer, allerdings werden die Neuerungen selten von den Verantwortlichen eingesetzt. Um für die bestehenden und kommenden Sicherheitslücken gewappnet zu sein, bedarf es eines Patch Managements, mit dem systematisch Sicherheitsupdates in allen IT-Systemen installiert werden können. Technische Sicherheitsmaßnahmen müssen risikoorientiert und systematisch die Gefahren und Risiken der Einrichtungen abdecken und entsprechend geplant werden.

1.5.1 BSI-Grundschutz überarbeitet

Im Oktober 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen überarbeiteten IT-Grundschutz vorgestellt. Alle Bestandteile wurden grundlegend überarbeitet und an die geänderten Rahmenbedingungen angepasst.
Die Neuausrichtung des IT-Grundschutzes war aus Sicht des BSI notwendig geworden, da der Grundschutz verschlankt und gerade auf kleinere und mittlere Unternehmen stärker fokussiert werden sollte. Um diesem Umstand Rechnung zu tragen, hat das BSI die Systematik des Grundschutzes geändert. Die bisherigen Standards der Reihe 100 wurden durch die überarbeiteten Standards der Reihe 200 ersetzt. Gleichzeitig wurden neue Themen wie Cloud, Internet of Things und industrielle Kontrollsysteme in den Grundschutz integriert.

Die Umsetzung des Grundschutzes sieht jetzt drei Stufen der Umsetzung und damit der Absicherung einer Einrichtung vor: Basis-Absicherung, Standard-Absicherung und eine Absicherung für erhöhten Schutzbedarf.

Mit der neuen Basis-Absicherung können die Einrichtungen schnell und mit überschaubarem Aufwand die wichtigsten Schutzmaßnahmen ergreifen. Dann kann darauf aufbauend die Standard-Absicherung erreicht werden.

Diese neuen Bausteine können auch auf Einrichtungen der katholischen Kirche adaptiert werden, was aus Sicht des Katholischen Datenschutzzentrums zu begrüßen wäre. Der neue IT-Grundschutz und alle dazugehörigen Dokumente können auf der Internetseite des BSIs (https://bsi.bund.de) heruntergeladen werden.

1.5.2 Standard-Datenschutzmodell

Das Standard-Datenschutzmodell (SDM) ist ein von den Datenschutzaufsichtsbehörden des Bundes und der Länder entwickeltes Werkzeug, mit dem die Schutzanforderungen der DSGVO operationalisiert werden können.[2]

Das SDM kann dazu beitragen, die notwendigen Maßnahmen für ein dem Risiko angemessenes Schutzniveau im Sinne von Art. 32 Abs. 1 DSGVO bzw. § 26 Abs. 1 KDG zu ergreifen und zu dokumentieren. Gleichzeitig kann es für die regelmäßige Überprüfung und Fortentwicklung der ergriffenen Maßnahmen eingesetzt werden und so den in Art. 32 Abs. 1 Satz 1 Buchst. d) DSGVO bzw. § 26 Abs. 1 Satz 2 Buchst. d) KDG geforderten kontinuierlichen Verbesserungsprozess der Maßnahmen abbilden.

Art. 5 DSGVO bzw. § 7 KDG formulieren wesentliche Grundsätze für die Verarbeitung personenbezogener Daten: Die Verarbeitung muss rechtmäßig, nach Treu und Glauben, nachvollziehbar, zweckgebunden, auf das notwendige Maß beschränkt, auf der Basis richtiger Daten, vor Verlust, Zerstörung und Schädigung geschützt und die Integrität und Vertraulichkeit wahrend, stattfinden. Das SDM stellt geeignete Mechanismen zur Verfügung, um diese rechtlichen Anforderungen der DSGVO bzw. des KDG in konkrete technische und organisatorische Maßnahmen umzusetzen.

Aus den genannten rechtlichen Anforderungen werden die Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit abgeleitet.

"Das SDM stellt geeignete Mechanismen zur Verfügung, um diese rechtlichen Anforderungen der DSGVO bzw. des KDG in konkrete technische und organisatorische Maßnahmen umzusetzen."

2 Einzelheiten siehe „Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele", Version 1.1 vom April 2018.

Mit Hilfe dieser Gewährleistungsziele werden die rechtlichen Anforderungen der DSGVO bzw. des KDG in die gesetzlich geforderten technischen und organisatorischen Maßnahmen überführt. Damit kann das SDM den verantwortlichen Stellen standardisierte Maßnahmenkataloge zur Verfügung stellen, mit denen getroffene Maßnahmen auf ihre Wirksamkeit und ausreichenden Schutz überprüft werden können.

Gleichzeitig können die Datenschutzaufsichten aus dem SDM einheitliche Beratungs- und Prüfkonzepte entwickeln. Dies hat für die verantwortlichen Stellen den Vorteil, dass das SDM so zu einer transparenten datenschutzrechtlichen Bewertung durch die Datenschutzaufsicht führen kann und die Bewertung einer risikoorientierten Betrachtung einer Verarbeitung personenbezogener Daten durch die Datenschutzaufsicht für die verantwortliche Stelle nachvollziehbarer wird.

Das SDM richtet sich damit einerseits an die Stellen, die für die Verarbeitung personenbezogener Daten verantwortlich sind. Diese können mit dem SDM die erforderlichen Funktionen und Schutzmaßnahmen systematisch planen, umsetzen und kontinuierlich überwachen. Gleichzeitig bietet das Modell den Datenschutzaufsichten die Grundlage, um mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren, belastbaren Gesamturteil über ein Verfahren und dessen Komponenten zu gelangen.

Derzeit liegt das Dokument „Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele“ in der Version 1.1 vom April 2018 vor. Neben der stetigen Weiterentwicklung des Modells liegt der Schwerpunkt derzeit auf der Erarbeitung der konkreten Maßnahmenkataloge zu den einzelnen Themen. Erst mit diesen Maßnahmenkatalogen kann das Modell einfach in die Praxis umgesetzt werden.

1.5.3 WLAN-Verschlüsselung nach WPA2-Standard

Drahtlose Netzwerke sind in dem heutigen Alltag unverzichtbar geworden. Sie werden im privaten Bereich ebenso wie im geschäftlichen Umfeld genutzt. Nachdem die älteren WLAN-Verschlüsselungsstandards WEP und WPA aus Sicherheitsgründen schon länger nicht mehr verwendet werden sollten, galt die Nutzung von WLAN bei der Verwendung der aktuellen WPA2-Verschlüsslung bisher als sicher.

Forschern der Katholischen Universität Leuven ist es gelungen, den verschlüsselten Datentransfer mitzulesen und gegebenenfalls zu manipulieren. Grund ist eine Designschwäche von WPA2, bei dem die Entwickler den jetzt gezeigten Angriffsvektor nicht berücksichtigt haben. Bei WPA2 wird einem neuen Gerät im WLAN ein neuer Sicherheitsschlüssel auf Basis der WPA2-Verschlüsselung zur Verfügung gestellt. Mithilfe des jetzt aufgezeigten Angriffs bringt der Angreifer das neue

Gerät im WLAN dazu, für die Verschlüsselung einen vom Angreifer bereitgestellten schon benutzten Schlüssel zu verwenden. Da der Angreifer nun den genutzten Schlüssel kennt, kann er die Daten im WLAN von diesem Gerät mitlesen.

Die Hersteller von WLAN-Hardware können aber durch eine Art Filter den Angriff unterbinden. WLAN-Geräte sollten daher Firmware-Updates durchführen, um diesen Angriff nicht mehr zu ermöglichen.

1.5.4 USB Anschluss - praktisch, aber auch ein mögliches Sicherheitsrisiko

Der „Verizon 2016 Data Breach Investigations Report" wies dem USB-Anschluss (Universal Serial Bus) den Platz drei bei Datenlecks zu.

Jeder PC, jedes Tablet oder Smartphone besitzt in der Regel mindestens einen dieser USB-Anschlüsse, die durch entsprechende Gerätschaften wie USB-Sticks oder USB-Festplatten als Einfallstor von Kriminellen missbraucht werden können. Die kleinen Geräte sind für den schnellen Datenaustausch einfach zu nutzen, bieten aber besonders deshalb eine große Wahrscheinlichkeit des Verlusts. Durch die technischen Möglichkeiten der USB-Schnittstelle ist es sogar möglich, Schadsysteme in vorhandene Geräte, wie Tastatur oder Maus, zu integrieren. So schöpft der Anwender keinen Verdacht. Die IT-Sicherheit der Einrichtung ist womöglich in Gefahr.

"Ein mögliches Angriffsszenario besteht aus einem präparierten USB Stick, auf dem sich ein Schadcode befindet."

Ein mögliches Angriffsszenario besteht aus einem präparierten USB-Stick, auf dem sich ein Schadcode befindet. Beispielsweise ist an den „besitzerlosen" USB-Stick auf dem Parkplatz zu denken, der dort vom Angreifer „verloren" wurde.

Eine andere Angriffssituation wäre ein modifiziertes USB-Gerät, das vom Angreifer an das Endgerät (PC, Smartphone o.ä.) gesteckt wird. Durch die Simulation einer falschen USB-Kennung wird der Treiber automatisch vom Betriebssystem installiert. Dies geschieht auch bei gesperrten Systemen. Dieser Angriff ist als „Poisontap" bekannt. In diesem Szenario wird ein USB-Netzwerkadapter vorgegaukelt und das WPAD-Protokoll (Web Proxy Autodiscovery Protocol) missbraucht, welches zum Auffinden eines Web Proxys innerhalb des Netzwerks verwendet wird. Zum Aufrufen der vermeintlichen WPAD-Konfigurationsdatei werden die Benutzerdaten verlangt, der NTLM-Hash. Ist der Angreifer im Besitz dieses Hashes, kann er ihn zum Angriff nutzen, um sich so als legitimer Benutzer auszuweisen. Dieser Pass-the-Hash-Angriff ist insbesondere aus dem Angriff auf die IT des deutschen Bundestags bekannt geworden. Zum anderen kann der Angreifer durch Brute-Force Attacken das Kennwort entschlüsseln. Hierzu sind lediglich Zeit und Rechenkapazitäten der begrenzende Faktor.

Eine weitere Angriffsmöglichkeit wäre, dass der Angreifer eine Tastatur so modifiziert, dass sie bis zu 60 Tastaturanschläge pro Sekunde automatisch als Eingabe an den Rechner schickt. In dieser Geschwindigkeit bekommt das Opfer diese Eingaben gar nicht mit oder kann nicht schnell genug eingreifen. Auch kann dieser Angriff zur Entsperrung von Displaysperren von Smartphones genutzt werden.

Welche Möglichkeiten gibt es, diese Angriffe zu verhindern oder zumindest zu erschweren?

Bei diesen Überlegungen sollte der Nutzer an erster Stelle stehen. Durch regelmäßige Schulungen und Informationen sollte das Bewusstsein für diese Problematik geschärft und Risiken und Lösungsmöglichkeiten aufgezeigt werden.

Als eine mögliche Abwehrstrategie, kann die Nutzung von privaten USB-Geräten (USB-Sticks etc.) mit Hilfe von Dienstanweisungen ausgeschlossen werden. Technisch kann dies durch die Sperrung von USB-Ports über die Gruppenrichtlinien von Windows unterstützt und umgesetzt werden. Für die Verwendung von USB-Datenträgern sollte ein sogenannter LifeCycle erarbeitet und implementiert werden. Feste Vorgehensweisen bei Verlust und auch Entsorgung von nicht mehr benötigten Geräten sind dabei vorzugeben. Im Weiteren sollte die Boot-Reihenfolge der Systeme so angepasst sein, dass das Endgerät nicht alternativ über USB gestartet werden kann.

USB-Datenträger sollten nur verschlüsselt verwendet werden, so können bei Verlust die darauf befindlichen Daten nicht von Unbefugten genutzt werden. Die USB-Anschlüsse an den Endgeräten müssen geschützt werden. Ist der PC länger unbeaufsichtigt, muss der Zugang verhindert werden oder der PC heruntergefahren werden. Steht der PC an öffentlichen Orten, muss mechanisch oder über Gruppenrichtlinien der USB-Anschluss gesperrt werden.

Die Härtung des Betriebssystems sollte ebenfalls betrachtet werden. Ein funktionierendes Update- und Patch-Management sind hier notwendig.

Der Nutzer darf auch keine lokalen Administratorenrechte besitzen, um nicht einzelne Schutzmaßnahmen umgehen zu können. Durch weitere Maßnahmen, wie lokale Virenscanner oder Firewall, kann das Risiko weiter minimiert werden.

2 Die Datenschutzaufsicht in der katholischen Kirche

2.1 Struktur der Datenschutzaufsicht

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

Das Stichwort: Urteil des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsichten

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 9. März 2010 (Rechtssache C-518/07) entschieden, dass die nach der Datenschutz-Richtlinie 95/46/EG einzurichtenden nationalen Datenschutzaufsichten ihre Arbeit „in völliger Unabhängigkeit" ausüben können müssen. Dies bedeutet nach der Auslegung des EuGH, dass die Arbeit „ohne äußere Einflussnahme" wahrgenommen werden kann. Diese Unabhängigkeit schließe nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen.[3]

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

Die Verteilung ist in der nachfolgenden Übersicht dargestellt:

"Dieser Diözesandatenschutzbeauftragte nimmt die Funktion wahr, die im staatlichen Bereich der Landesdatenschutzbeauftrage als Datenschutzaufsicht wahrnimmt."

3 EuGH, Urteil vom 09.03.2010, Rs C-518/07, Rn. 30

Datenschutzaufsichten der katholischen Kirche Deutschlands

2.2 Konferenz der Datenschutzbeauftagten

Zu den Aufgaben des Diözesandatenschutzbeauftragten gehört gemäß § 18 Abs. 4 KDO das Hinwirken auf die Zusammenarbeit mit den anderen Diözesandatenschutzbeauftragten (zukünftig zu finden in § 44 Abs. 3 lit. f KDG).

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

Im Berichtszeitraum fanden zwei jeweils zweitägige Konferenzen im Mai in Freising und im November in Bremen statt. Neben der Beratung aktueller Fragestellungen waren die Begleitung des Gesetzgebungsverfahrens zur Umsetzung der Anforderungen der Europäischen Datenschutz-Grundverordnung in kirchliches Recht und die Vorbereitung

der sich daraus ergebenden Umsetzungsbedarfe für die kirchlichen Stellen wichtige Beratungspunkte der Sitzungen. Die Beschlüsse der Sitzungen sind in diesem Bericht in Kapitel 7 dokumentiert.

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

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

3 Aus der Tätigkeit des Datenschutzzentrums

3.1 Aufgabenkatalog (Beratung – Prüfung – Schulung)

Die betrieblichen Datenschutzbeauftragten in den Einrichtungen sind die ersten Ansprechpartner zu Datenschutzfragen vor Ort. Sie kennen die Einrichtung, die Prozesse und die handelnden Personen. Sie können als Anlaufstelle vor Ort schnell und unkompliziert helfen und sind so auf der ersten Stufe eine interne Stelle, die auf die Einhaltung des Datenschutzes achtet. Daneben gibt es den Diözesandatenschutzbeauftragten als von der Einrichtung unabhängige Datenschutzaufsicht.

Die Aufgaben des Diözesandatenschutzbeauftragten sind in der KDO bzw. ab Mai 2018 im KDG beschrieben. Wer der Ansicht ist, dass bei der Erhebung, Verarbeitung oder Nutzung - im KDG zukünftig unter dem Begriff „Verarbeitung" zusammengefasst - von personenbezogenen Daten durch eine (katholische) kirchliche Stelle datenschutzrechtliche Regelungen verletzt worden sind, kann sich gemäß § 15 KDO (zukünftig § 48 KDG) an den Diözesandatenschutzbeauftragten wenden. Dieser prüft den Sachverhalt und hört dazu die betroffene kirchliche Stelle an, soweit nach dem Vortrag ein Verstoß gegen datenschutzrechtliche Regelungen vorliegen könnte. Wichtig ist dabei das Benachteiligungsverbot des § 15 Abs. 3 KDO (zukünftig § 48 Abs. 3 KDG): „Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an den Diözesandatenschutzbeauftragten gewendet hat." Wer sich an den Diözesandatenschutzbeauftragten wendet, darf daher keine Nachteile erleiden.

Die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben gehört nicht nur im Rahmen der Beschwerdebearbeitung, sondern als allgemeine Kernaufgabe zu den Tätigkeiten des Diözesandatenschutzbeauftragten (vgl. § 18 Abs. 1 KDO, zukünftig § 44 Abs. 1 KDG).

Hierzu führt er anlassbezogen, auf Grund der bei ihm 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 der KDO und der KDO-DVO (Datensicherheit). Beide Komponenten, die Umsetzung der rechtlichen Vorgaben und der technisch-organisatorischen Schutzmaßnahmen, müssen beachtet und umgesetzt werden, damit Datenschutz wirksam werden kann und die Betroffenen den gesetzlich vorgesehenen Schutz genießen können.

Kommt die Datenschutzaufsicht im Rahmen einer Prüfung oder der Bearbeitung einer Beschwerde zu dem Ergebnis, dass ein bestimmter von der kirchlichen Stelle durchgeführter oder unterlassener Vorgang bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu beanstanden ist, wird dies dokumentiert und der verantwortlichen Stelle schriftlich mitgeteilt. Je nach Schwere des Verstoßes gegen die datenschutzrechtlichen Vorgaben, kann das Katholische Datenschutzzentrum eine angemessene Frist zur Behebung der Abweichungen von den gesetzlichen Vorgaben setzen. Mit Inkrafttreten des neuen KDG im Mai 2018 wird die Datenschutzaufsicht noch weitergehende Befugnisse erhalten, um Verstößen gegen die gesetzlichen Bestimmungen abzuhelfen.

Um datenschutzrechtlichen Verstößen vorzubeugen, steht das Team des Katholischen Datenschutzzentrums im Rahmen seiner Aufgaben beratend zur Verfügung, um als Referent oder mit schriftlichen Informationen allgemeine Hinweise zur Umsetzung des Datenschutzes zu geben oder im Wege der Beratung im Einzelfall weiterzuhelfen.

Durch das Inkrafttreten des neuen KDG und die damit einhergehenden nötigen Veränderungen und Vorbereitungen gab es im zweiten Halbjahr des Jahres 2017 einen großen Bedarf an Informationen, so dass das Katholische Datenschutzzentrum bei vielen Veranstaltungen kirchlicher Stellen Vorträge zum Thema „Aus KDO wird KDG“ für verschiedene Gruppen von Multiplikatoren (u. a. betriebliche Datenschutzbeauftragte, Einrichtungsleitungen, Fachverantwortliche, IT-Verantwortliche, Mitarbeitervertretungen) gehalten hat. Auf Grund des kurzen Umsetzungszeitraums für das neue Gesetz bis Ende Mai 2018 wird es im ersten Halbjahr des Jahres 2018 weiterhin viele Vorträge in diesem Bereich geben.
Bedingt durch die stetig zunehmende Sensibilisierung der kirchlichen Stellen und der Betroffenen für den Umgang mit personenbezogenen Daten, nahmen im Berichtszeitraum sowohl die Beratungsanfragen als auch die Beschwerden zu. Gerade im Bereich der Beratungsanfragen war zusätzlich eine enorme Zunahme durch die Unsicherheiten bei der Umsetzung der kommenden neuen Regelungen des kirchlichen Datenschutzes zu verzeichnen.

Insgesamt betrachtet, machen die Beratungsvorgänge immer noch den größten Anteil an den bearbeiteten Vorgängen aus. Dies wird noch verstärkt durch die gestiegene Anzahl von Informationsveranstaltungen, auf denen das Katholische Datenschutzzentrum als Referent vertreten war und die ebenfalls beratenden Charakter haben.

3.2 (Vor-Ort-) Prüfungen und Prozessaufnahmen

Neben den Prüfungen, die im schriftlichen Verfahren auf Grund von Beschwerden Betroffener durchgeführt wurden, hat das Katholische Datenschutzzentrum im Jahr 2017 auch sechs anlasslose Vor-Ort-Prüfungen in kirchlichen Einrichtungen vorgenommen. Dabei wurde in jeder Diözese unseres Zuständigkeitsbereiches mindestens eine kirchliche Stelle überprüft. Bei der Auswahl der Einrichtungen sollte ein möglichst großes Spektrum der Einrichtungsformen abgedeckt werden. So wurde eine Kirchengemeinde, ein Verwaltungszentrum einer Kirchengemeinde, ein Caritasverband, eine Schule, ein Krankenhaus und eine Fortbildungsakademie überprüft. Die Auswahl der Einrichtungen erfolgte nach dem Zufallsprinzip.

"Insgesamt betrachtet, machen die Beratungsvorgänge immer noch den größten Anteil an den bearbeiteten Vorgängen aus."

Die Prüfungen erfolgten anlasslos und wurden mit den Einrichtungen abgestimmt. Bei den Terminen standen das gegenseitige Kennenlernen und die Beratung der Einrichtung im Vordergrund. Dabei wurden die allgemeine Umsetzung der datenschutzrechtlichen Vorgaben nach der Anordnung über den kirchlichen Datenschutz (KDO) und der Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) in einem beratenden Gespräch überprüft. Neben den grundlegenden Vorgaben wie die Bestellung eines betrieblichen Datenschutzbeauftragten, Umgang und Häufigkeit von Mitarbeiterschulungen, der Umgang mit Einwilligungen, der Erstellung und Pflege von Verfahrensverzeichnissen, der Einsatz von Auftragsdatenverarbeitung wurden die in § 6 KDO geforderten technischen und organisatorischen Maßnahmen evaluiert.

Sofern sich aus dem Gespräch entsprechender Handlungsbedarf ergab, wurde den kirchlichen Stellen im Nachgang zu den Terminen ein Maßnahmenplan zu Verfügung gestellt, für deren Abarbeitung auch Erledigungstermine vereinbart waren. Für das Katholische Datenschutzzentrum ist hier wichtig, mit diesen anlasslosen Prüfungen immer wieder einen aktuellen Stand zur Umsetzung des Datenschutzes vor Ort zu erhalten und die täglichen Probleme im Umgang mit personenbezogenen Daten am praktischen Beispiel geschildert zu bekommen.

Die Ergebnisse aus den anlasslosen und anlassbezogenen Prüfungen zeigen, dass in allen Bereichen eine positive Wahrnehmung des Datenschutzes festgestellt werden konnte, wenn auch im Detail noch Vebesserungsbedarf besteht, wie die Beschwerden der Betroffenen zeigen. Die Ausführungen und Umsetzungen der gesetzlichen Vorgaben sind jedoch auf unterschiedlichem Niveau vorzufinden. Hier ist vor allem immer wieder erkennbar, dass nur die ausreichende Beschäftigung mit dem Thema und die damit verbundene Bereitstellung der notwendigen Ressourcen an verschiedenen Stellen (IT, Fachabteilungen, betrieblicher

Datenschutz) die gewünschten Ergebnisse bietet. Die Umsetzung des Datenschutzes kann gelingen, wenn auf die Notwendigkeiten im Alltag der Einrichtung mit Zeit und Mitteln reagiert werden kann und die Beschäftigung mit dem Thema durch Einbindung in die Prozesse der Einrichtungen zum normalen Tagesgeschäft wird.

Neben den anlasslosen Prüfungen von Einrichtungen wurden im Berichtszeitraum die (erz-)bischöflichen Generalvikariate besucht. Im Rahmen dieser Prozessaufnahmen wurde der Umgang mit personenbezogenen Daten an den verschiedenen Stellen dieser zentralen Kirchenverwaltungen aufgenommen. Im Mittelpunkt stand auch hier das gegenseitige Kennenlernen und die Beantwortung von Fragen zum Datenschutz.

Auch die Ergebnisse aus den Prozessaufnahmen zeigen, dass der Datenschutz in den (erz-)bischöflichen Generalvikariaten positiv umgesetzt wird. Der Ausbau der Stellen der betrieblichen Datenschutzbeauftragten als erste Ansprechpartner vor Ort wird diesen Trend positiv verstärken und beschleunigen.

3.3 Einzelne Themen beleuchtet

Nachfolgend möchten wir einige Themenbereiche aus den Anfragen, Beschwerden und Prüfungen darstellen, da diese Sachverhalte Bedeutung über den Einzelfall hinaus haben.

3.3.1 Auftrags(daten)verabeitung

Bestehende Rechtslage nach der KDO
Sehr viele Anfragen an das Katholische Datenschutzzentrum bezogen sich auf Verträge mit Dienstleistern. Oft wurde um eine Stellungnahme gebeten, ob ein bestimmter Vertrag oder Vertragsentwurf mit den Bestimmungen des § 8 KDO in Einklang steht.

Das Katholische Datenschutzzentrum kann aber eine einzelfallbezogene rechtliche Prüfung konkreter Vertragsentwürfe nicht vornehmen. Gleichwohl haben wir die Anfrager insofern unterstützt, als dass wir die Anforderungen der KDO als auch des KDG wiederholt erläutert haben. Die Frage, ob eine vorgesehene Verfahrensweise datenschutzrechtlich in Ordnung ist, könnte daher unter Vorlage des konkreten Vertrages beantwortet werden, nicht aber ob ein Vertragsentwurf (in Gänze) rechtskonform ist.

Neben der Benennung von Gegenstand, Zweck, Beginn und Ende bzw. Dauer der Verarbeitung muss auch der betriebliche Datenschutzbeauftragte des Auftragnehmers benannt werden. Weitere notwendigen Angaben sind die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen. Das Prozedere zum Zustandekommen

von Unterauftragsverhältnissen muss klar geregelt werden, wobei dem Auftraggeber ein Widerspruchsrecht einzuräumen ist. Zu Vertragsbeginn bestehende Unteraufträge müssen benannt werden.

Eine häufige Anmerkung unseres Hauses war, dass die Pflichten des Auftragnehmers, z. B. zur Umsetzung technischer und organisatorischer Maßnahmen, oft nur allgemein und nicht hinreichend konkret benannt wurden. Weiterhin fehlte oft die Verpflichtung des Auftragnehmers zur weitestgehenden Unterstützung des Auftraggebers bei der Erfüllung von Betroffenenrechten, also z. B. des Rechtes auf Auskunft, Berichtigung und Löschung. Weiterhin muss der Auftragnehmer verpflichtet werden, im Fall von Prüfungen durch die Aufsichtsbehörde mit dieser zusammenzuarbeiten und deren Mitarbeitern ein Betretungsrecht einzuräumen.

Zukünftige Rechtslage nach dem KDG

Die Anordnung über den kirchlichen Datenschutz (KDO), welche durch das Gesetz über den Kirchlichen Datenschutz (KDG) ab dem 24. Mai 2018 abgelöst wird, enthielt die bisherigen Vorgaben im Falle des Abschlusses einer Vereinbarung zur Auftragsdatenverarbeitung. Die in § 8 KDO niedergelegten Anforderungen entsprachen den vergleichbaren Regelungen des Bundesdatenschutzgesetzes (BDSG). Die Neuregelung in § 29 KDG orientiert sich an der Europäischen Datenschutz-Grundverordnung (DSGVO).

§ 29 KDG enthält gegenüber dem bisherigen Recht umfassendere Vorgaben und schärfer formulierte Anforderungen. War es bisher erforderlich, dass der Verantwortliche seinen Auftragsdatenverarbeiter sorgfältig auswählt, so fordert § 29 KDG nunmehr, dass nur mit Auftragsverarbeitern zusammengearbeitet wird, die hinreichende Garantien dafür bieten, dass die Bearbeitung im Einklang mit dem KDG erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird, insbesondere durch die geeigneten technischen und organisatorischen Maßnahmen, welche der Auftragsverarbeiter durchzuführen hat. Deutlicher als bisher wird der Bereich der Unterauftragsverhältnisse angesprochen. § 29 Absatz 2 KDG stellt klar, dass weitere Auftragsverarbeiter nicht ohne vorherige Genehmigung des Verantwortlichen durch den ursprünglichen Auftragsverarbeiter eingesetzt werden dürfen. Dies wird verbunden mit einer Informationspflicht im Falle von Änderungen.

Entsprechend den vertragsgestaltenden Möglichkeiten, welche die DSGVO in diesem Bereich einräumt, hat die Verarbeitung durch den Auftragsverarbeiter entweder auf Grundlage eines Vertrags oder eines anderen in § 29 Absatz 3 KDG aufgeführten Rechtsinstruments zu erfolgen. Die Vereinbarung dazu ist gemäß § 29 Absatz 9 KDG schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Dabei sind die Formvorschriften des Bürgerlichen Gesetzbuchs (BGB) der Bundesrepublik Deutschland zu beachten. Die Vorgaben für den

Vertragsinhalt sind in den Absätzen 3 und 4 des § 29 KDG ausführlicher als bisher aufgeführt. Gleiches gilt für die Inanspruchnahme eines weiteren Auftragsverarbeiters durch den ursprünglichen Auftragsverarbeiter gemäß § 29 Absatz 5 KDG. Zu den Bestandteilen der vertraglichen Vereinbarung gehört z. B. die Verpflichtung des Auftragsverarbeiters, alle in § 26 KDG beschriebenen technischen und organisatorischen Maßnahmen zu ergreifen. Weiterhin wird stärker die Unterstützungsleistung betont, die der Auftragsverarbeiter für den Verantwortlichen erbringen soll.

Anders als bisher lediglich in der Durchführungsverordnung zur KDO ist nunmehr im Gesetz selbst in § 29 Absatz 11 KDG festgelegt, in welchen Ländern eine Datenverarbeitung durch den Auftragsverarbeiter zulässig ist. Dabei ist der Bereich zunächst auf die Mitgliedstaaten der Europäischen Union sowie auf den Europäischen Wirtschaftsraum beschränkt. Abweichungen sind jedoch unter den in der vorgenannten Vorschrift aufgeführten Voraussetzungen zulässig.

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands hat die Praxishilfe „Auftragsverarbeitung nach dem Kirchlichen Datenschutz (KDG)“ herausgegeben, auf die an dieser Stelle hingewiesen wird und die auf der Internetseite des Katholischen Datenschutzzentrums abrufbar ist.

3.3.2 Videoüberwachung

Auch im vergangenen Jahr wurde das Katholische Datenschutzzentrum mehrfach mit Fragen rund um das Thema der Videoüberwachung befasst. Die vorgetragenen Fällen lassen auf eine Unsicherheit der verantwortlichen Stellen schließen, welche Bewertungen im Vorfeld einer Entscheidung pro oder contra einer Videoüberwachung vorzunehmen sind und wann die in der KDO genannten Voraussetzungen für eine Zulässigkeit erfüllt sind.

Bereits im Jahresbericht 2016[4] haben wir die im Zusammenhang mit der Videoüberwachung verwendeten Begriffe und die grundsätzlich vorzunehmenden Abwägungen nach § 5a KDO erläutert. Demnach ist gemäß § 5a Abs. 1 Nr. 1 KDO eine Beobachtung zulässig, wenn sie zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder nach § 5a Abs. 1 Nr. 2 KDO zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Die Zulässigkeit ist aber in beiden Varianten dann nicht gegeben, wenn bei einer Interessenabwägung die Interessen des Betroffenen überwiegen.

Gerade der Aspekt der Erforderlichkeit musste in mehreren Fällen besonders erörtert werden: Erforderlich ist eine Maßnahme dann, wenn ihr Zweck [z. B. der Schutz des Überwachenden oder anderer Perso-

4 Jahresbericht 2016, Kapitel 3.2.1

nen vor Eingriffen in Leib, Leben oder Eigentum (z. B. Einbruch, Diebstahl, Vandalismus) und die Ermöglichung straf- und zivilrechtlicher Verfolgung solcher Eingriffe durch die Strafverfolgungsbehörden] durch andere, weniger gravierende, wirtschaftlich, technisch und organisatorisch zumutbare Maßnahmen nicht erreicht werden kann. Eine Videoüberwachung ist demnach nur zulässig, wenn der Betreiber im Vorfeld andere Maßnahmen (z. B. einbruchssichere Schlösser und Fenster, regelmäßige Kontrollgänge, spezielle Oberflächenbeschichtungen zum Schutz gegen Graffiti etc.) erwogen oder sogar erprobt hat und sich diese Maßnahmen als nicht geeignet erweisen.

Diese Erwägungen gelten nicht nur für die Abwehr von Gefahren. So haben wir in einem Fall, in dem ein Einrichtungsbetreiber den Empfangsbereich eines Gästehauses video-beobachten wollte, damit Mitarbeiter in einem rückwärtigen Büro die ankommenden Gäste bemerken können, die Installation einer einfachen Klingel-Taste vorgeschlagen.

Weitere Fälle betrafen die Kenntlichmachung der Beobachtung nach § 5a Abs. 2 KDO. Danach ist nicht nur der Umstand der Beobachtung, sondern auch die verantwortliche Stelle erkennbar zu machen. Damit ist klar, dass das Anbringen der oft vom Hersteller der Video-Überwachungsanlage mitgelieferten Aufkleber „Achtung Videoüberwachung“ nicht ausreicht, sondern der Verantwortliche der Überwachung explizit genannt werden muss.

"Die Zulässigkeit ist ... dann nicht gegeben, wenn bei einer Interessenabwägung die Interessen des Betroffenen überwiegen."

3.3.3 Bring-Your-Own-Device (BYOD)

Unter dem Schlagwort „Bring-Your-Own-Device“ (BYOD) wird verstanden, dass Mitarbeiter ihr eigene persönliche Hardware – typischerweise Laptops, Tablets oder Mobiltelefone – für dienstliche Anwendungen wie z. B. Email, Intranet oder sonstige meist portalgestützte Applikationen, aber auch normale Telefonate nutzen und damit in die betriebliche Infrastruktur einbringen.

Dieses Vorgehen bedingt i. d. R. mehr oder weniger Softwareinstallation auf dem privaten Gerät und verlangt deshalb gut konzeptionierte Sicherheitsmaßnahmen zur Trennung der dienstlichen von der privaten Umgebung auf dem Endgerät, damit IT-Sicherheit und Datenschutz gewährleistet bleiben.

Ausgehend von der Annahme, dass nahezu jeder Mitarbeiter heute über private Endgeräte verfügt, die aus technischer Sicht auch für dienstliche Zwecke eingesetzt werden könnten, liegt der Vorteil von BYOD für Mitarbeiter (besonders für Mitarbeiter im mobilen Einsatz) vor allem darin, dass kein zusätzliches (dienstliches) Endgerät mitgeführt werden muss und die gewohnte Bedienung des privaten Gerätes auch für dienstliche Zwecke fortgesetzt werden kann. Für den Dienstgeber entfällt die

Investition in Hardware, wenn dem Mitarbeiter stattdessen eine pauschale Nutzungsentschädigung gezahlt wird.

Das Katholische Datenschutzzentrum wurde mehrfach um eine Beurteilung von BYOD-Szenarien im kirchlichen Umfeld gebeten. Aus datenschutzrechtlicher Sicht ist eine datenschutz-konforme Lösung bei der Verschmelzung privater und dienstlicher Nutzung auf einem einzigen Gerät, sei es nun ein privates oder ein dienstliches Gerät, nur mit großem Aufwand zu organisieren.

In der Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) wird in Punkt IV (Zu § 6 KDO), Anlage 2, Punkt 3.4 (Mindestanforderungen) ausgeführt: „Es ist sicherzustellen, dass auf dienstlich genutzten Anlagen der elektronischen Datenverarbeitung ausschließlich autorisierte Programme zu dienstlichen Zwecken verwendet werden. Die Benutzung privater Programme ist unzulässig." Und in Punkt 5.1. derselben Anlage heißt es: „Die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungssystemen zu dienstlichen Zwecken ist grundsätzlich unzulässig." Nur unter strengen Voraussetzungen kann der Dienststellenleiter eine Ausnahme von diesem Grundsatz genehmigen, die dann aber schriftlich begründet werden muss.

Auch wenn sich der Punkt IV der KDO-DVO streng genommen nur auf „Arbeitsplatz-Computer" bezieht, wird man doch vernünftigerweise die Bestimmungen auch auf den Einsatz von „mobilen Computern", also u. a. Laptops, Tablets und Smart-Phones, anwenden müssen.

An anderer Stelle der KDO-DVO, in den „IT-Richtlinien zur Umsetzung" des Punktes IV, Anlage 2, wird in Punkt 4.3 bestimmt, dass die Genehmigung zur Nutzung privater Geräte für die dienstliche Verarbeitung von personenbezogenen Daten zwingend voraussetzt, dass sich der Eigentümer einem Gerätemanagement (MDM – Mobile Device Management) durch die dienstliche Stelle unterwirft, d. h. die Dienststelle ist berechtigt, Programme und Daten (auch private!) zu löschen, wenn dies zur Wahrung von Datenschutzbestimmungen notwendig ist.

Alle diese Bestimmungen zusammengenommen schließen eine vernünftige parallele dienstliche und private Nutzung auf einem einzigen Gerät ohne weitere Maßnahmen wie z. B. Container-Lösungen o. ä. aus.

Es bleibt abzuwarten, ob sich durch zukünftige technische Entwicklungen eine deutliche, durchgehende und transparent zu managende Trennung (etwa im Sinne einer Virtualisierung) zwischen mehreren Umgebungen auf einer einzigen Hardware implementieren lässt, was dann zu einer Neubewertung der BYOD-Frage führen könnte.

3.3.4 Unerlaubte Weitergabe von personenbezogenen Daten

Adressdaten, Geburtsdaten oder Informationen über religiöse oder ethnische Zugehörigkeiten werden im alltäglichen Leben oft einfach weitergegeben. Dabei sollte stets im Vorfeld über den Zweck der Weitergabe nachgedacht werden und somit die schutzwürdigen Interessen des Betroffenen im Vordergrund stehen. Eine Weitergabe ist - soweit die KDO anwendbar ist - nur dann rechtmäßig, wenn diese auf eine Rechtsgrundlage gestützt werden kann.

Unter anderem trat im Jahr 2017 eine Petentin an das Katholische Datenschutzzentrum mit dem Anliegen heran, dass sie trotz erklärtem Werbewiderspruch postalische Schreiben zu verschiedenen Werbeaktionen bekam. Die Petentin hatte sich im Vorfeld absichern wollen und der entsprechenden Stelle schriftlich mitgeteilt, dass sie eine Nutzung ihrer Daten in keiner Weise duldet, diese somit auch nicht - durch Speicherung - verarbeitet werden dürfen.

Ihre Beschwerde richtete sie an das Katholische Datenschutzzentrum, da sie trotzdem mehrfach Werbematerial durch die entsprechende Stelle zugesandt bekam. Von Seiten des Katholischen Datenschutzzentrums wurde dieses Vorgehen kritisiert und die entsprechende Stelle aufgefordert, ihre administrativen Vorgänge so zu strukturieren, dass eine Speicherung und anschließende Weitergabe von personenbezogenen Daten in einem vergleichbaren Fall nicht mehr vorkommen kann.

Dies ist nur eine der zahlreichen Möglichkeiten, personenbezogene Daten unerlaubt weiterzugeben. Wie schnell ist es passiert, dass der Bildschirm des Computers am Arbeitsplatz nicht gesperrt ist, sodass ein Zugriff auf die gespeicherten Daten durch Dritte möglich ist, obwohl man nur kurz das Büro verlässt. Auch der Verlust von Datenträgern, wie portable Speichermedien (USB-Sticks) oder Laptops ist ein Datenverlust und stellt eine - möglicherweise - unerlaubte Weitergabe dar.

Durch die neue Vorschrift zur Datenschutz-Folgenabschätzung (siehe Art. 35 DSGVO und § 35 KDG) ist der Verantwortliche gesetzlich verpflichtet, im Vorfeld eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten vorzunehmen. Dabei können eventuelle Schwachstellen in vielen Fällen durch technische und/oder organisatorische Maßnahmen ohne großen Aufwand vermieden werden, sodass es nicht zu einer Meldung an die Datenschutzaufsicht kommen muss. Die Aufgabe der Risikoanalyse obliegt dabei der jeweiligen verantwortlichen Stelle.

"Eine Weitergabe ist - soweit die KDO anwendbar ist - nur dann rechtmäßig, wenn diese auf eine Rechtsgrundlage gestützt werden kann."

3.3.5 Umgang mit Krankmeldungen im Arbeitsverhältnis

Das Katholische Datenschutzzentrum hatte sich im Berichtszeitraum auch mit mehreren Beschwerden zum Umgang mit Krankmeldungen / Arbeitsunfähigkeitsbescheinigungen zu befassen. Hierbei richteten sich die Beschwerden gegen den Meldeweg der Krankmeldung.

So war in einer Einrichtung festgelegt, dass die Arbeitsunfähigkeitsbescheinigungen an den unmittelbaren Vorgesetzten zu senden bzw. übergeben waren. Der Vorgesetzte gab die Arbeitsunfähigkeitsbescheinigungen dann an die Personalabteilung weiter. Als Begründung wurde von den kirchlichen Einrichtungen vorgetragen, dass die Vorgesetzten unmittelbar über die Erkrankung unterrichtet werden müssten.

Das Katholische Datenschutzzentrum hat diese Praxis insoweit beanstandet, als die Vorgesetzten bei den Arbeitsunfähigkeitsbescheinigungen nicht nur die Tatsache der Erkrankung an sich und die voraussichtliche Dauer der Erkrankung erkennen können. Auf der Bescheinigung ist auch der Name und die Fachrichtung des behandelnden Arztes angegeben. Dies sind aber Informationen, die für den direkten Vorgesetzten nicht notwendig sind.

Das Katholische Datenschutzzentrum hat daher in diesen Fällen mit der betroffenen Einrichtung abgesprochen, dass die Bescheinigung wieder der Personalabteilung direkt zugesendet wird. Die Personalabteilung informiert dann die Vorgesetzten über den Umstand der Erkrankung und die voraussichtliche Dauer. Weitere aus der Bescheinigung ersichtliche Details bleiben nur der Personalstelle bekannt.

"Jede Person bekommt den Zugriff auf die Daten, die sie zur Erfüllung der ihr zugewiesenen Aufgaben benötigt."

Dies ist ein Beispiel dafür, dass auch innerhalb einer kirchlichen Einrichtung nicht alle Personen über alle personenbezogenen Daten informiert sein müssen bzw. darauf Zugriff haben dürfen. Jede Person bekommt den Zugriff auf die Daten, die sie zur Erfüllung der ihr zugewiesenen Aufgaben benötigt.

3.3.6 Cloud Nutzung

Das Katholische Datenschutzzentrum erhielt in dem Berichtszeitraum einige Anfragen zur Nutzung von IT-Infrastruktur außerhalb der verantwortlichen Stelle. Dies kann die Nutzung von "Software as a Service" bis zur Nutzung von "Infrastructure as a Service" beinhalten. Auftragnehmer waren sowohl Unternehmen aus der freien Wirtschaft als auch Einrichtungen innerhalb der katholischen Kirche. Hierzu gilt zu beachten, dass die KDO-DVO eine Auftragsverarbeitung ausschließlich im Geltungsbereich des BDSG erlaubt. Dies wird jedoch nicht von Unternehmen erfüllt, die den Zugriff von außerhalb der Europäischen Union ermöglichen. Als Beispiel können hier Microsoft Office 365 oder Amazon AWS

genannt werden. Diese Einschränkung betrifft nicht nur das Betreiben der Anwendung, sondern auch einen möglichen Support Zugriff.

Bei der Verwendung von sogenannten Cloud Dienstleistungen muss die verantwortliche Stelle die technischen und organisatorischen Schutzmaßnahmen auch bei dem Dienstleister überprüfen, da die Datenhoheit weiterhin in seinem Verantwortungsbereich liegt. Diese Überprüfung kann sowohl durch eine Vor-Ort Prüfung, als auch durch weitere Alternativen wie Zertifikaten erfolgen.

Ein Ausfall des Dienstleisters, zum Beispiel durch eine Insolvenz, muss bei einer Auslagerung der Daten mit berücksichtigt werden. Hierzu ist eine Exit Strategie im Rahmen der Risikobewertung erforderlich.
Als Fazit lässt sich zusammenfassen, dass eine Auslagerung von diversen IT Produkten eine Entlastung der angespannten IT-Abteilung mit sich bringen mag, aber nicht die Verantwortung des Datenschutzes an den Dienstleister überträgt. Je nach Vertragsgegenstand ist der Abschluss eines Vertrages, in dem alle Merkmale einer Auftragsverarbeitung beschrieben sind, notwendig.

3.3.7 Datenschutz in Kirchengemeinden

In den Kirchengemeinden gibt es immer wieder größere Unsicherheiten im Umgang mit personenbezogenen Daten. Besonders die Veröffentlichung von bestimmten Ereignissen, wie Trauungen, Taufen, Sterbefällen oder auch Ehejubiläen etc. in Aushängen, Pfarrbriefen und Kirchenzeitungen und auch auf der Internetpräsenz der Gemeinde wurde oft in Fragestellungen im vergangenen Jahr thematisiert.

"Unabdingbar ist der Abschluss eines Vertrages in dem alle Merkmale einer Auftragsverarbeitung beschrieben sind."

Die derzeit geltenden Ausführungsrichtlinien für den pfarramtlichen Bereich geben vor, welche Daten unter welchen Voraussetzungen durch kirchliche Publikationsorgane und im Internet veröffentlicht werden dürfen.

In den Ausführungsrichtlinien für den pfarramtlichen Bereich wird unterschieden, ob es sich um kirchliche Amtshandlungen (z. B. Taufen, Erstkommunion, Firmung, Trauung, Weihen und Exequien) oder besondere Ereignisse (z. B. Alters-und Ehejubiläen, Geburten, Sterbefälle, Ordens-und Priesterjubiläen) handelt. Bei beiden ist die Veröffentlichung von Name, Vorname und Datum in kirchlichen Publikationsorganen (z. B. Aushang oder Pfarrbrief) zulässig, wobei bei den besonderen Ereignissen einmal jährlich in geeigneter Form darauf hinzuweisen ist, dass der Betroffene vorab der Veröffentlichung in den gedruckten Pfarrnachrichten widersprechen kann.

Eine Veröffentlichung im Internet bedarf stets der Einwilligung des Betroffenen, um seine personenbezogenen Daten zu schützen. Sperrvermerke sind in jedem Fall zu beachten.

3.3.8 Einwilligungen

Um die Verarbeitung personenbezogener Daten in zulässiger Weise durchführen zu können, wird in vielen Fällen auf die Einwilligung der betroffenen Person als Rechtsgrundlage zurückgegriffen. An eine solche Einwilligung sind jedoch gesetzlich festgelegte Anforderungen zu stellen. Sind diese nicht erfüllt, liegt keine wirksame Einwilligung und damit keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten vor.

Welchen Voraussetzungen eine Einwilligung unterliegt und wann diese wirksam erteilt werden kann, war im Berichtszeitraum mehrfach Gegenstand von Anfragen.

Die Einwilligung wird in § 3 KDO (bzw. zukünftig in § 8 KDG) näher beschrieben. Eine wirksame Einwilligung muss freiwillig ohne jeglichen Zwang und schriftlich abgegeben werden und explizit auf den Einzelfall abstellen. Das bedeutet konkret, dass der betroffenen Person bewusst sein muss, dass sie ihre Daten nicht mitteilen und einer Verarbeitung nicht zustimmen muss. Für die Erteilung einer wirksamen Einwilligung bedarf es nicht der Geschäftsfähigkeit, sondern es genügt die Urteils- und Einsichtsfähigkeit des Betroffenen. Sind jedoch Persönlichkeitsrechte oder wirtschaftliche Interessen betroffen (Bilder oder Videos; Zahlung von Mitgliedsbeiträgen) ist die Einwilligung des Betroffenen und (soweit erforderlich) des gesetzlichen Vertreters/Betreuers einzuholen.

"Eine wirksame Einwilligung muss freiwillig ohne jeglichen Zwang und schriftlich abgegeben werden und explizit auf den Einzelfall abstellen."

Wird beabsichtigt, die Daten an Dritte zu übermitteln, so muss die Art und der Zweck der Übermittlung angegeben werden. Soll die Einwilligung besondere Arten von personenbezogenen Daten (vgl. § 2 Abs. 10 KDO) umfassen, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen. Die Einwilligungserklärung muss auf den jeweiligen Zweck zugeschnitten sein. Generelle Einwilligungen für nicht näher genannte Zwecke und für alle Verarbeitungen in der Zukunft sind nicht wirksam. Nicht zu vergessen ist, dass im Text der Einwilligung auf die Möglichkeit des Widerrufs hingewiesen werden muss.

3.3.9 Erweitertes Führungszeugnis

Um Vorkommnissen sexualisierter Gewalt vorzubeugen und damit Kinder, Jugendliche und schutzbedürftige Erwachsene zu schützen, gibt es seit Inkrafttreten zum 1. Mai 2010 das 5. Gesetz zur Änderung des Bundeszentralregistergesetzes vom 16. Juli 2009. Dort ist in § 30a und § 31 BZRG die Möglichkeit eröffnet, durch das Verlangen der Vorlage eines erweiterten Führungszeugnisses solche Bewerber vor der Einstellung auszusortieren, die entsprechende - sie ausschließende - Voreintragungen im Bundeszentralregister aufweisen.

Was steht im erweiterten Führungszeugnis?
Das erweiterte Führungszeugnis gibt auch Auskunft über solche Sexualdelikte, welche in dem einfachen normalen polizeilichen Führungszeugnis nicht aufgeführt sind, weil die Rechtsfolgen der Taten zu geringfügig ausgefallen sind. Gerade diese Information ist jedoch von enormer Bedeutung für den Arbeitgeber, der zum Beispiel eine neue Erzieherin oder einen neuen Erzieher einstellen möchte.

Wie läuft die praktische Umsetzung?
Zunächst ist zwischen mindestens drei Bereichen zu differenzieren. Für den weltlichen als auch für den kirchlichen Bereich gelten die Vorschriften der Sozialgesetzbücher. Im kirchlichen Bereich, gerade im Bereich der Gemeindearbeit, gilt zudem die Präventionsordnung.

1. § 72a SGB VIII
In § 72a SGB VIII ist für den Bereich der Jugendhilfe geregelt, dass für Hauptamtliche die Vorlagepflicht gilt (Abs. 1). Aus Abs. 5 ergibt sich, dass bei Neben- und Ehrenamtlichen nur Einsicht in das erweiterte Führungszeugnis genommen und lediglich der Umstand der Einsichtnahme, das Datum dieser und ob eine Voreintragung besteht, dokumentiert werden dürfen. Da sich Abs. 5 nur auf die erhobenen Daten aus den Absätzen 3 und 4 bezieht und es dort um die Neben- und Ehrenamtlichen geht, wird daraus geschlossen, dass die bloße Einsichtnahme vom Gesetzgeber abschließend nur für die Neben- und Ehrenamtlichen gewollt ist. Für die Hauptamtlichen (Abs. 1) gilt der Vorlagebegriff aus Absatz 1.

2. § 75 Abs. 2 SGB XII
In § 75 Abs. 2 SGB XII, welcher für den Bereich der Sozialhilfe gilt, wurde neu geregelt, dass sich die Träger ebenfalls ein erweitertes Führungszeugnis gemäß § 30 BZRG vorlegen lassen müssen. In dieser Regelung, welche an dieser Stelle erst seit dem 1. Januar 2017 existiert, wird
- anders als im Bereich der Jugendhilfe- nicht zwischen Neben-, Ehren- und Hauptamtlichen differenziert. Es wird sogar eindeutig klargestellt, dass der Träger der Einrichtung nur den Umstand der Einsichtnahme, das Datum des Führungszeugnisses und die Information, ob die das Führungszeugnis betreffende Person wegen einer in Satz 3 genannten Straftat rechtskräftig verurteilt worden ist, speichern darf.
3. §124 Abs. 2 S. 3 SGB IX
In § 124 Abs. 2 S. 3 SGB IX, welcher eine Regelung für den Bereich der Eingliederungshilfe für Menschen mit Behinderung darstellt, ist ebenfalls vorgesehen, dass die dort beschäftigten (ehrenamtlichen) Personen das erweiterte Führungszeugnis vorlegen. Zur Dokumentation und Aufbewahrung gilt das unter Punkt 2 Gesagte.

4. Präventionsordnung
In der Ordnung zur Prävention gegen sexualisierte Gewalt an Minderjährigen und schutz-oder hilfebedürftigen Erwachsenen (Präventionsordnung PrävO) ist geregelt, dass für kirchliche Rechtsträger und ihre

Dienststellen, Mitarbeitende sowie ehrenamtlich Tätige, ein erweitertes Führungszeugnis vorlegen müssen, welches nach Ablauf von 5 Jahren jeweils wiederholt werden muss. Diese Regelung greift demnach über den Anwendungsbereich der zwei bereits genannten Normen hinaus. Sie ist jedoch stets nachrangig zu bewerten, wenn ein erweitertes Führungszeugnis aufgrund der zuvor genannten Vorschriften der Sozialgesetzbücher (§ 72a SGB VIII, § 75 Abs. 2 SGB XII, und § 124 Abs. 2 S. 3 SGB IX) einzuholen ist, da in diesen Fällen entsprechend der Punkte 1 bis 3 vorzugehen ist. Ob eine Einsicht und Dokumentation genügt, ist nicht geregelt. Demnach können die Träger dies selbst entscheiden.

Zudem ist einmalig eine Selbstauskunftserklärung dahingehend vorzulegen, dass der Mitarbeitende nicht wegen einer einschlägigen Tat verurteilt und auch insoweit kein Ermittlungs- oder Voruntersuchungsverfahren gegen ihn eingeleitet worden ist. Zudem ist er verpflichtet, den Rechtsträger über die Einleitung eines Ermittlungsverfahrens in Kenntnis zu setzen.

3.3.10 Messenger Dienste

Die Konferenz der Diözesandatenschutzbeauftragten hat mit Beschluss vom 3./4. Mai 2017 festgestellt, dass die dienstliche Nutzung von Messengerdiensten wie z. B. WhatsApp datenschutzrechtlich nicht immer unbedenklich möglich ist. Wenn z. B. bei der Nutzung des Messengers das Telefonbuch auf dem mobilen Endgerät an den Betreiber des Dienstes übermittelt wird, um dem Nutzer Kommunikationspartner aus dem Telefonbuch vorschlagen zu können, dann bedarf es für diese Übermittlung der personenbezogenen Daten einer Rechtsgrundlage, die regelmäßig fehlen wird. Für eine derartige Datenverarbeitung wird der Nutzer in der Regel keine Einwilligung von allen Personen, deren Nummern sich in dem Telefonbuch befinden, eingeholt haben.

Als weiterer Grund für die Beurteilung der Konferenz ist die Verschlüsselung der Daten, welche zwischen zwei Geräten ausgetauscht werden, zu nennen. Sind diese nicht sicher vor dem Zugriff Unberechtigter geschützt, liegt kein sicherer Datenaustausch vor.

4 Vorbereitung auf das neue KDG

Zum 24. Mai 2018 tritt das Gesetz über den Kirchlichen Datenschutz (KDG) in Kraft. Auch wenn die Grundprinzipien des Datenschutzes und viele Begriffe und Instrumente gleichbleiben, bringt das KDG in Anlehnung an die Europäische Datenschutzgrundverordnung einige Änderungen mit sich, auf die sich die kirchlichen und caritativen Einrichtungen in Nordrhein-Westfalen einstellen müssen.

Mit Inkrafttreten des KDG werden voraussichtlich erheblich mehr kirchliche Einrichtungen verpflichtet sein, einen betrieblichen Datenschutzbeauftragten zu benennen. Die Umsetzung eines gesetzeskonformen Datenschutzes bleibt auch unter der Geltung des KDG die Aufgabe des Verantwortlichen, also der Leitung der Einrichtung. Als Teil der Führungsaufgabe ist die Leitung einer Einrichtung für die Umsetzung und Bereitstellung der benötigten Mittel und Ressourcen verantwortlich.

4.1 Benennung eines betrieblichen Datenschutzbeauftragten (bDSB)

Künftig müssen die Diözesen, Kirchengemeinden und Kirchengemeindeverbände - unabhängig von der Zahl ihrer hauptamtlichen und ehrenamtlichen Mitarbeiter - einen betrieblichen Datenschutzbeauftragten benennen. Dies gilt auch für die Gliederungen und Fachverbände der Caritas, unabhängig von ihrer Rechtsform und die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und sonstigen kirchlichen Rechtsträger unabhängig von Ihrer Rechtsform, wenn ihre Kerntätigkeit in der umfangreichen regelmäßigen und systematischen Überwachung von Personen oder in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht. Darüber hinaus ist ein betrieblicher Datenschutzbeauftragter zu benennen, wenn mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten befasst sind. Hierbei sind auch ehrenamtliche Helfer mit Zugang zu diesen Daten mitzuzählen.

"Jede kirchliche Einrichtung sollte daher umgehend prüfen, ob sie zur Benennung eines betrieblichen Datenschutzbeauftragten ab dem 24. Mai 2018 verpflichtet ist."

Das KDG nennt in den §§ 36 ff KDG Vorgaben und Voraussetzungen für die Benennung, die organisatorische Einbindung der Funktion, der Beendigung der Tätigkeit und zu den Kompetenzen des betrieblichen Datenschutzbeauftragten und seiner Aufgabenwahrnehmung.

Jede kirchliche Einrichtung sollte daher umgehend prüfen, ob sie zur Benennung eines betrieblichen Datenschutzbeauftragten ab dem 24. Mai 2018 verpflichtet ist. Die Verpflichtung kann sowohl mit der Benennung eines internen, wie auch eines externen Datenschutzbeauftragten erfüllt werden. Ebenso kann für mehrere Verantwortliche ein gemeinsamer (externer) Datenschutzbeauftragter benannt werden.
Für die benannten Datenschutzbeauftragten ist zu prüfen, wie

- die Fachkunde des betrieblichen Datenschutzbeauftragten sichergestellt werden kann,
- ausreichende Ressourcen und Mittel für die Arbeit bereitgestellt werden können und
- eine Vertretungsregelung für den betrieblichen Datenschutzbeauftragten gestaltet werden kann.

4.2 Bestandsaufnahme der Verarbeitungsprozesse mit personenbezogenen Daten

Schon die derzeit noch geltende KDO kennt in § 3a KDO die Verpflichtung der verantwortlichen Stelle zur Erstellung eines Verfahrensverzeichnisses für die Verfahren der automatisierten Datenverarbeitung.
§ 31 KDG erweitert dieses Verzeichnis, das nun „Verzeichnis von Verarbeitungstätigkeiten" heißt, auf alle Verarbeitungstätigkeiten des Verantwortlichen im Zusammenhang mit personenbezogenen Daten und präzisiert auch den Inhalt der Dokumentation. Auftragsverarbeiter sind nun gesetzlich verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten für die Auftragsverarbeitungen zu führen und dies dem Auftraggeber auch zur Verfügung zu stellen.

Die Verpflichtung zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gilt nach § 31 Abs. 5 KDG für alle Einrichtungen mit 250 oder mehr Beschäftigten oder bei Einrichtungen mit weniger als 250 Beschäftigten, wenn durch die Verarbeitung die Rechte und Freiheiten der Betroffenen gefährdet werden, die Verarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung besondere Datenkategorien gemäß § 11 KDG oder Daten über strafrechtliche Verurteilungen nach § 12 KDG beinhaltet.

Um ein genaueres Verständnis davon zu bekommen, mit welchen Daten in der Einrichtung umgegangen wird, sollte ein Ist-Zustand der Datenverarbeitung erhoben werden.
Die Einrichtungen sollten daher prüfen,

- welche Verfahren / Prozesse vorhanden sind, in denen personenbezogene Daten verarbeitet werden,
- ob für die aktuell genutzten Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, schon eine Dokumentation in Form des Verfahrensverzeichnisses vorliegt und
- ob für weitere Verfahren ein Verzeichnis erstellt werden muss. Zur Eruierung können die in einem Qualitätsmanagementsystem beschriebenen Prozesse herangezogen werden.

4.3 Verträge und Dienstvereinbarungen überprüfen

Je nach Aufgabe der kirchlichen Einrichtung und Funktion bei der konkreten Verarbeitung der personenbezogenen Daten sind an der Verarbeitung auch Dienstleister beteiligt oder es sind Verträge mit den Auftraggebern, Auftragnehmern oder Kunden geschlossen worden.

Auch wenn die Grundzüge des Datenschutzrechts beim Wechsel von der KDO zum KDG weiter Anwendung finden, so müssen die bestehenden Verträge doch daraufhin überprüft werden, ob die vertraglichen Regelungen noch den Anforderungen der neuen gesetzlichen Vorgaben entsprechen. Gleiches gilt für die vorhandenen Dienstvereinbarungen, soweit sie Regelungen enthalten, die die Verarbeitung personenbezogener Daten regeln.
Einrichtungen sollten daher prüfen, ob

- bestehende Verträge an die neuen Regelungen angepasst werden müssen.
- vorhandene Dienstvereinbarungen geändert werden müssen.
- als Folge der Änderung der Verträge bzw. Dienstvereinbarungen die Verarbeitungsübersicht ergänzt werden muss.

4.4 Besonderen Schutz von Kindern und Jugendlichen sicherstellen

Da Kinder und Jugendliche nicht bei allen Angeboten die Risiken für ihre (Persönlichkeits)Rechte immer vollständig überblicken können, schützt das KDG die Kinder und Jugendlichen bei den Angeboten, bei denen die Verarbeitung personenbezogener Daten auf Basis einer Einwilligung erfolgen soll. Hier stellt das Gesetz eine differenzierte Lösung zur Verfügung, die unter bestimmten Voraussetzungen die Einwilligung der Sorgeberechtigten erfordert, bei anderen kirchlichen Beratungsangeboten aber die Einwilligung des Kindes oder des Jugendlichen ausreichen lässt.

Einrichtungen sollten daher prüfen, ob

- sie Angebote mit einer elektronischen Beratung für Kinder und Jugendliche anbieten. Falls ja, ist zu prüfen, ob geeignete technische Maßnahmen zur Feststellung des Alters ergriffen werden müssen.
- andere Angebote, die nicht primär auf Kinder und Jugendlichen ausgerichtet sind, aber von diesen Zielgruppen häufig genutzt werden, ebenfalls angepasst werden müssen.

4.5 Betroffenenrechte umsetzen

Dem zunehmenden Umfang und der zunehmenden Komplexität der Verarbeitung personenbezogener Daten hat der europäische Gesetzge-

ber die Rechte der Betroffenen gegenübergestellt. Diese Rechte sollen den Betroffenen die Möglichkeit geben, sich über die Verarbeitung ihrer Daten bei den verarbeitenden Stellen zu informieren und diese Verarbeitung in gewissem Umfang auch beeinflussen zu können.
Die Rechte der Betroffenen werden durch die Vorschriften der §§ 14 bis 25 KDG in Übereinstimmung mit der Europäischen Datenschutzgrundverordnung erweitert und in den Fokus gerückt. Das gilt vor allem für das Recht auf Löschung von Daten (§ 19 KDG) und das Recht auf Datenübertragbarkeit (§ 22 KDG), aber auch für die Informationspflichten des Verantwortlichen an die Betroffenen.

Betroffene sind in transparenter Weise, d. h. in einfacher und klarer Sprache, über die Verarbeitung ihrer Daten präzise, verständlich und in leicht zugänglicher Form zu informieren. Insbesondere sind die Informationen so zur Verfügung zu stellen, dass sie auch für Minderjährige oder Menschen mit Hilfebedarf verständlich sind.

"Insbesondere sind die Informationen so zur Verfügung zu stellen, dass sie auch für Minderjährige oder Menschen mit Hilfebedarf verständlich sind."

Neu ist das Recht auf Datenübertragbarkeit in elektronischen Verfahren, bei dem der Betroffene die Möglichkeit hat, seine Daten von einem Verantwortlichen an einen anderen Verantwortlichen zu übermitteln.
Einrichtungen sollten daher prüfen, ob

- sie einen umfassenden Überblick haben, in welchen Prozessen welche Daten welcher Betroffenen verarbeitet werden. Nur so kann später eine vollständige Auskunft erteilt werden. Die Verarbeitungsübersichten sind hierbei eine wichtige Informationsquelle und sollten daher immer aktuell und vollständig sein,
- sie präzise, verständlich und ausreichend über die Datenverarbeitung informieren,
- sie alle Betroffenenrechte auch technisch umsetzen können. So müssen z. B. die genutzten Systeme zur Datenverarbeitung das Löschen von Daten auch zulassen.

4.6 Datenschutzkonzept erstellen oder vervollständigen

In einem Datenschutzkonzept werden die für eine datenschutzrechtliche Beurteilung notwendigen Informationen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschrieben. In dem Konzept wird die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten geregelt. Das Datenschutzkonzept hat das Ziel, eine zusammenfassende Dokumentation der datenschutzrechtlichen Maßnahmen und Richtlinien einer Einrichtung darzustellen. Es kann als Grundlage für datenschutzrechtliche Prüfungen wie Datenschutz-Audits oder Prüfungen der Aufsicht dienen, da hiermit die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden kann.Inhalte sollten sein:

- Festlegung und Dokumentation der obersten Datenschutzziele der Einrichtung. Die Datenschutzziele orientieren sich an den Daten-

schutz-Grundsätzen, die jede Einrichtung individuell an die Gegebenheiten anpasst.
- Festlegung von Rollen und Verantwortlichkeiten (Vertretungsregelung, betriebliche Datenschutzbeauftragte, Datenschutz-Koordinatoren etc.).
- Prozesse zu einer kontinuierlichen Verbesserung des Datenschutzmanagements in der Einrichtung.
- Schulung, Sensibilisierung und Verpflichtung der Mitarbeiter.
- Dokumentation spezifischer gesetzlicher Regelungen oder Verhaltensregeln, die für den Umgang mit personenbezogenen Daten in der Einrichtung gelten.
- Dokumentation des Schutzbedarfes der Daten, Festlegung von Datenkategorien und den damit verbundenen Sicherheitsvorkehrungen.
- Dokumentation von internen und externen Prüfungen und der Erkenntnisse daraus.
- Beschreibung der technischen und organisatorischen Maßnahmen, die die Einrichtung umgesetzt hat.

4.7 Verfahrensverzeichnis wird aufgewertet

Im neuen KDG sind - wie auch in der Europäischen Datenschutzgrundverordnung - im Vergleich zu den bisher geltenden Gesetzen einige Begrifflichkeiten angepasst worden. So wurde auch der Begriff der Verfahrensverzeichnisse durch den Begriff „Verzeichnis von Verarbeitungstätigkeiten“ (kurz Verarbeitungsverzeichnis) abgelöst.

Neben der Umbenennung der Übersicht gibt es aber auch noch inhaltliche Änderungen. Es entfällt z. B. die Meldepflicht an den Diözesandatenschutzbeauftragten, wenn kein betrieblicher Datenschutzbeauftragter benannt wurde und auch die Führung eines sog. Jedermanns-Verzeichnisses.

Die allgemeine Nachweis- und Dokumentationspflicht für die Datenverarbeitungen wird bei dem Verantwortlichen verankert (§ 31 Abs. 1 KDG). Darüber hinaus sind mit dem KDG jetzt auch die Auftragsverarbeiter zur Führung eines Verarbeitungsverzeichnisses verpflichtet für die Verarbeitungen, die sie im Auftrag ausführen.

Die Dokumentation der Verarbeitungsprozesse in den Einrichtungen bleibt eine wichtige Aufgabe und ist die Grundlage für die Dokumentation der gesetzeskonformen Verarbeitung von personenbezogenen Daten. Dies gilt insbesondere vor dem Hintergrund der nun eingerichteten erweiterten Sanktionsmaßnahmen der Datenschutzaufsicht bis hin zur Verhängung eines Bußgeldes (§ 51 KDG).

Die Verzeichnisse von Verarbeitungstätigkeiten dienen nicht nur als Nachweis gegenüber der Aufsichtsbehörde, sondern bilden auch eine

der Grundlagen bei der Erfüllung der Pflichten gegenüber den Betroffenen (z. B. Informations- und Transparenzpflichten aus den §§ 14 bis 25 KDG).

Die bei der Verarbeitung der personenbezogenen Daten getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten sind auch weiterhin ein Kernstück der Dokumentation. Hier ist z. B. aufzuführen, wie Pseudonymisierung, Verschlüsselung, Rechteverwaltung, einschließlich Lese- und Bearbeitungsbefugnis, Datensicherungsmaßnahmen, Wiederherstellbarkeit oder die Belastbarkeit des Systems umgesetzt bzw. sichergestellt werden.

Spätestens bis zum Ablauf der Übergangfrist des 30.06.2019 sind KDG-konforme Verarbeitungsübersichten zu erstellen oder bestehende Verzeichnisse anzupassen (vgl. § 57 Abs. 4 KDG).

Einrichtungen sollten daher prüfen,

- inwieweit die bereits vorhandenen Verfahrensverzeichnisse den neuen Vorgaben entsprechen und diese gegebenenfalls anpassen.
- ob für weitere Verarbeitungstätigkeiten eine Verarbeitungsübersicht erstellt werden muss.

4.8 Möglichkeit zur Vornahme einer Datenschutz-Folgenabschätzung einrichten

Die Datenschutz-Folgenabschätzung ist ein Instrument, um das Risiko zu erkennen und zu bewerten, das für die Rechte und Freiheiten des Betroffenen durch den Einsatz einer bestimmten Verarbeitungstechnologie oder des Systems entsteht. Die Datenschutz-Folgenabschätzung wird die bisher vorzunehmende Vorabkontrolle (§ 6 KDO) ersetzen. Sie ist für bestimmte, risikobehaftete Verarbeitungstätigkeiten durchzuführen (§ 35 Abs. 2 KDG).

Im Rahmen einer Datenschutz-Folgenabschätzung soll eine Abwägung der Risiken erfolgen, die die geplante Verarbeitung der personenbezogenen Daten der Betroffenen auf deren Rechte und Freiheiten hat. Sofern hierbei hohe Risiken festgestellt werden, sind entsprechende Maßnahmen zur Senkung der Risiken zu ergreifen.

Als eine erste Hilfestellung zum Umgang mit diesem Instrument der Risikoabwägung haben die Diözesandatenschutzbeauftragten die Praxishilfe 11 „Datenschutz-Folgenabschätzung nach dem Kirchlichen Datenschutzgesetz (KDG)“ herausgegeben.
Die Ausgestaltung der Datenschutz-Folgenabschätzung ist zweigeteilt. Zum einem besteht sie aus der Risikoanalyse und zum anderen aus den zu ergreifenden bzw. ergriffenen Maßnahmen zur Verminderung bzw. zum Ausschluss der Risiken. Die Durchführung der Datenschutz-Folgenabschätzung obliegt dem Verantwortlichen.

Einrichtungen sollten daher prüfen, ob

- zukünftig bei der Einführung eines neuen Verfahrens eine Datenschutz-Folgenabschätzung durchzuführen ist,
- für die Durchführung einer Datenschutz-Folgenabschätzung die notwendigen Prozesse vorgesehen sind und die Ressourcen und Mittel für die Durchführung zur Verfügung stehen,
- die durch die Verarbeitung von Daten entstehenden Risiken in ein vorhandenes Risikomanagement aufgenommen werden sollen.

4.9 Haftung und Schadenersatz

Im kirchlichen Bereich ist nun in § 50 KDG auch die zivilrechtliche Haftung für das Entstehen materieller und immaterieller Schäden zu Lasten der betroffenen Personen geregelt. Eine ausdrückliche betragsmäßige Haftungsbeschränkung ist nicht vorgesehen. Mehrere Ersatzpflichtige (z. B. Einrichtung und Auftragsverarbeiter) haften als Gesamtschuldner. Einrichtungen sollten daher prüfen, ob

- die mögliche Haftung und ein möglicher Schadenersatz in ein bestehendes Risikomanagement aufzunehmen sind,
- in der Einrichtung bereits Prozesse oder Verfahren existieren, die den Umgang mit Haftungsansprüchen regeln,
- bestehende Versicherungen über die neuen Haftung- und Schadenersatzvoraussetzungen zu informieren sind.

5 Das Katholische Datenschutzzentrum

5.1 Zuständigkeitsbereich

Das Katholische Datenschutzzentrum ist für die fünf nordrhein-westfälischen (Erz-)Diözesen zuständig. Diese sind von der Fläche deckungsgleich mit dem Bundesland Nordrhein-Westfalen. Hinzu kommen noch einzelne Gemeinden oder Teile von Gemeinden in Rheinland-Pfalz, die zum Erzbistum Köln gehören, und in Niedersachsen und in Hessen, die zum Erzbistum Paderborn gehören. In diesem Gebiet leben knapp sieben Millionen Menschen römisch-katholischen Glaubens (Stand 2016).

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

5.2 Aufbau der Einrichtung

Das Katholische Datenschutzzentrum ist eine eigenständige Körperschaft des öffentlichen Rechts. Die Körperschaft des öffentlichen Rechts wurde gegründet von den Erzdiözesen Köln und Paderborn und den Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil). In den Verwaltungsrat des Katholischen Datenschutzzentrums haben die (Erz)Bischöfe ihre jeweiligen Generalvikare entsandt. Der Vertreter der Erzdiözese Paderborn, Herr Generalvikar Hardt, wurde vom Verwaltungsrat zum Vorsitzenden des Gremiums gewählt. Die Geschäftsführung des Gremiums wurde dem Leiter des Katholischen Datenschutzzentrums übertragen.

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

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

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

	Soll	Ist
Leitung KDSZ / Diözesandatenschutzbeauftragter	1	1
Stellv. Leitung KDSZ / stellv. Diözesandatenschutzbeauftragter	1	1
Referentinnen / Referenten	5	4
Sachbearbeiterinnen / Sachbearbeiter	2	2
Sekretariat	2	2
Gesamt	**11**	**10**

Personalausstattung KDSZ zum 31.12.2017 (in Vollzeitstellen)

Bei der Planung des Katholischen Datenschutzzentrums wurde konsequent auf die Umsetzung des Urteils des Europäischen Gerichtshofes vom 09.03.2010 zur Unabhängigkeit und Selbständigkeit der Datenschutzaufsichtsbehörden[5] geachtet und die Veränderungen durch die Europäische Datenschutzgrundverordnung bzw. deren Umsetzung in kirchliches Recht schon berücksichtigt.

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

Nach der Übernahme der Aufgaben des Diözesandatenschutzbeauftragten der fünf (Erz-)Diözesen in NRW zum 01.09.2016 galt es im Jahr 2017 sowohl das Katholische Datenschutzzentrum als Einrichtung aufzubauen und die Datenschutzaufsicht weiter auszubauen, wie auch die kirchlichen Stellen auf die anstehenden Veränderungen durch die neuen gesetzlichen Grundlagen vorzubereiten und zu unterstützen.

5 Siehe hierzu schon oben Kap. 2.1

Das Katholische Datenschutzzentrum hat im Berichtszeitraum sein Informationsangebot stetig erweitert und den Internetauftritt unter www.katholisches-datenschutzzentrum.de ausgebaut. Zusammen mit den anderen Diözesandatenschutzbeauftragten wurde eine gemeinsame Schriftenreihe (Praxishilfen) zum neuen kirchlichen Gesetz für den Datenschutz herausgegeben.

5.3 Finanzen

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

Für das Kalenderjahr 2017 hat der Verwaltungsrat des KDSZ auf Vorschlag des Diözesandatenschutzbeauftragten den Haushaltsplan in Höhe von 981.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben bewilligt.

Für das Folgejahr 2018 wird sich das genehmigte Budget auf Grund der dann erreichten Soll-Personalstärke auf 1.331.000 Euro erhöhen.

5.4 Vertretung in Gremien und Arbeitsgruppen in der katholischen Kirche

Das Katholische Datenschutzzentrum ist weiterhin mit einem Referenten in der Unterarbeitsgruppe der Ständigen Arbeitsgruppe Datenschutz- und Melderecht/IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands (VDD) vertreten. Diese Unterarbeitsgruppe hat 2016 / 2017 den Vorschlag für das neue kirchliche Datenschutzgesetz erarbeitet und kümmert sich derzeit um die Neufassung der Durchführungsverordnung zum neuen Datenschutzgesetz.

Bei der Weiterentwicklung der diözesanen Gesetze und der Diskussion von grundsätzlichen Rechtsfragen sind die Justitiarinnen und Justitiare der fünf (Erz-)Diözesen und der Justitiar des Katholischen Büros NRW in Düsseldorf die ersten Ansprechpartner des Katholischen Datenschutzzentrums. Das Katholische Datenschutzzentrum hält daher einen regelmäßigen Kontakt zu den Rechtsabteilungen der Generalvikariate und zum Katholischen Büro NRW.

5.5 Vernetzung

5.5.1 Vernetzung mit kirchlichen Stellen

Die Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen stehen in ständigem Austausch zu aktuellen Fragen und grundsätzlichen Themen. Die Besprechungen, Telefon- oder Videokonferenzen dienen diesem Austausch und der Vorbereitung und Verabschiedung gemeinsamer Beschlüsse.[6]

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

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

5.5.2 Vernetzung mit staatlichen Stellen

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

Diese Kontakte zu den staatlichen Stellen helfen vergleichbare Auslegungen der Gesetze bei vergleichbaren Vorgängen und damit ein vergleichbares Datenschutzniveau sicherzustellen. Diese Zusammenarbeit ist auch dann hilfreich, wenn es um den Datenaustausch zwischen kirchlichen und staatlichen oder nicht-öffentlichen Stellen im Sinne des Bundesdatenschutzgesetzes geht, da das Katholische Datenschutzzentrum nur die datenschutzrechtliche Bewertung für die kirchliche Stelle vornehmen kann.

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

6 Siehe Kapitel 2.2 dieses Berichtes zur Konferenz der Diözesandatenschutzbeauftragten und Kapitel 7 dieses Tätigkeitsberichtes zu den Beschlüssen der Konferenz.

5.6 Öffentlichkeitsarbeit

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

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 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. Das Katholische Datenschutzzentrum erstellt in unregelmäßigen Abständen einen Newsletter, der über die Internetseite abonniert werden kann. Viel Wert wurde unter anderem auf die Sicherheit gelegt, was z. B. auch ein gesichertes Kontaktformular beinhaltet. Über diese Kontaktmöglichkeit will das Katholische Datenschutzzentrum jedem Beteiligten die gesicherte Kontaktaufnahme ermöglichen.

Eine deutliche Steigerung gab es im Berichtszeitraum bei den Anfragen nach Vorträgen durch das Katholische Datenschutzzentrum. Hierbei waren verschiedenste Gruppen und Formate vertreten. Bei diesen Informationsveranstaltungen ist das Katholische Datenschutzzentrum als Referent vertreten, organisiert die Veranstaltungen aber nicht selbst. Mit diesen Vorträgen konnten, gerade gegen Ende des Berichtszeitraumes, zum neuen Datenschutzgesetz der Kirche hunderte Multiplikatoren erreicht werden.

Der Informationsbedarf der kirchlichen Stellen, der Betroffenen und der Öffentlichkeit zum kirchlichen Datenschutz war im Berichtszeitraum unvermindert hoch. Durch die Verabschiedung des neuen Gesetzes über den Kirchlichen Datenschutz (KDG) verstärkte er sich noch einmal zum Jahresende hin.

6 Ausblick

Das Jahr 2017 stand noch im Zeichen des organisatorischen und personellen Aufbaus des Katholischen Datenschutzzentrums. Mittlerweile sind die organisatorischen Voraussetzungen geschaffen und die Personalsuche fast abgeschlossen.

Mit dem neuen Gesetz über den Kirchlichen Datenschutz (KDG) wird Ende Mai das neue kirchliche Datenschutzrecht für die Katholische Kirche in Deutschland in Kraft treten, welches die an die Europäische Datenschutz-Grundverordnung angepassten Regelungen enthält. Hier sehen wir einen enormen Beratungsbedarf in Bezug auf die neuen Regelungen und deren Umsetzung. Wir reagieren darauf mit der Ausweitung unseres Informationsangebotes, sowohl in schriftlicher Form, wie auch durch die Vorstellung der neuen Regelungen auf Informationsveranstaltungen durch unser Haus.

Daneben wird das Katholische Datenschutzzentrum zum 1. Januar 2018 auch die Aufsicht über den Verband der Diözesen Deutschlands (VDD) übernehmen. Der Verband der Diözesen Deutschlands ist Rechtsträger der Deutschen Bischofskonferenz. Neben der Hauptverwaltung des VDD in Bonn fallen damit auch die dem VDD direkt rechtlich zugehörigen Einrichtungen unter die Aufsicht des Katholischen Datenschutzzentrums, wie z. B. das Katholische Büro in Berlin.

Die Katholische Kirche Deutschlands feiert im Mai 2018 in Münster den 101. Katholikentag. Das Katholische Datenschutzzentrum wird unter Beteiligung der anderen katholischen Datenschutzaufsichten auf der Kirchenmeile seine Aufgaben und sein Angebot vorstellen und allen Besuchern für Gespräche zur Verfügung stehen. Weiterhin ist die Veranstaltung einer Podiumsdiskussion zu einem aktuellen Datenschutzthema geplant.

"Daneben wird das Katholische Datenschutzzentrum zum 01. Januar 2018 auch die Aufsicht über den Verband der Diözesen Deutschlands (VDD) übernehmen."

7 Anhang Beschlüsse der Konferenz der Diözesandatenschutz-beauftragten im Jahr 2017

7.1 Beschluss zur Nutzung von Messenger-diensten (Sitzung vom 3./4. Mai 2017 in Freising)

Nutzung von Messenger-Diensten

Die Konferenz der Diözesandatenschutzbeauftragten beschließt, dass die Verwendung eines Messenger-Dienstes zu dienstlichen Zwecken untersagt ist, soweit eine physikalische Datenspeicherung außerhalb des Gebietes des EWR und der Schweiz stattfindet oder keine Punkt-zu-Punkt-Verschlüsselung genutzt wird. Nach einem Jahr sollte die Rechtslage erneut überprüft werden.

Abkürzungsverzeichnis

BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfD EKD	Beauftragter für den Datenschutz der EKD
BGH	Bundesgerichtshof
DDSB	Diözesandatenschutzbeauftragter
DOK	Deutsche Ordensobernkonferenz
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSB	betrieblicher Datenschutzbeauftragter
DSG-EKD	Datenschutz der evangelischen Kirche in Deutschland
DSGVO	Europäische Datenschutzgrundverordnung
EKD	Evangelische Kirche in Deutschland
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
KDG	Gesetz über den Kirchlichen Datenschutz
KDO	Anordnung über den kirchlichen Datenschutz
KDO-DVO	Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz
KDSZ	Katholisches Datenschutzzentrum
LfD	Landesbeauftragter für den Datenschutz
LDI	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
SDM	Standard-Datenschutzmodell
VDD	Verband der Diözesen Deutschlands
VwVfG	Verwaltungsverfahrensgesetz

Hl. Ivo

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

Sein Gedenktag ist der 19. Mai.

Bildnachweis: 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