Jahresbericht 2016

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

Berichtszeitraum
01.09.–31.12.2016

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

Az. 0.7.01 / 01-2017

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

1. Jahresbericht

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

für den Zeitraum 01.09.2016 – 31.12.2016

vorgelegt im März 2017

Redaktionsschluss: 28. Februar 2017

Inhaltsverzeichnis

Vorwort

„Datenschutz 2.0“ ist ein Schlagwort, das die Entwicklungen der letzten Monate sehr treffend beschreibt.
Da ist zum einen das **Katholische Datenschutzzentrum.** Als unabhängige Körperschaft des öffentlichen Rechts hat es in der Person des Diözesandatenschutzbeauftragten, der zugleich Leiter der Einrichtung ist, die Datenschutzaufsicht für die Erzdiözesen Köln und Paderborn und die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) zum 01. September 2016 übernommen.
Im Rahmen des Selbstverwaltungsrechtes der Kirchen haben die fünf (Erz-)Diözesen mit der Konzentration der bisher dezentral in den fünf (Erz-)Diözesen wahrgenommenen Funktion des Diözesandatenschutzbeauftragten[1] eine zukunftsfähige Lösung für die Wahrnehmung dieser gesetzlichen Aufgabe zur Sicherung des Grundrechtes auf informationelle Selbstbestimmung des Art. 2 Abs. 1 GG geschaffen.
Mit der Gründung des Katholischen Datenschutzzentrums als unabhängige Körperschaft des öffentlichen Rechts wurde die Datenschutzaufsicht organisatorisch und personell neu aufgestellt – Datenschutz 2.0 eben.
Mit der Einrichtung der unabhängigen Körperschaft des öffentlichen Rechts setzten die fünf (Erz-)Diözesen auch die Forderungen aus einem Urteil des Europäischen Gerichtshofes aus dem Jahre 2010 um[2]. Der EuGH hatte in dem Urteil betont, dass „die für die Überwachung der Verarbeitung personenbezogener Daten […] zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt 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].
Die fünf (Erz-)Diözesen sind hier konsequent den notwendigen und richtigen Schritt für eine gesetzeskonforme und – auch im Hinblick auf die neuen Regelungen der EU-Datenschutzgrundverordnung – zukunftsfähige Lösung dieser wichtigen Aufgabe gegangen.

Zum anderen hat der europäische Gesetzgeber im Jahr 2016 nach vierjähriger Beratung die **Datenschutzgrundverordnung** verabschiedet.
Mit dem Instrument der europäischen Verordnung als unmittelbar geltendem Europarecht sollte eine möglichst umfassende Vereinheitlichung des Datenschutzrechts in Europa durch diese weitreichende Neugestaltung der datenschutzrechtlichen Regelungen erreicht werden – Datenschutz 2.0.
Für die katholische Kirche ist wichtig, dass in Art. 91 der DSGVO das Selbstverwaltungsrecht der Kirchen ausdrücklich anerkannt wird. Damit verbunden

[1] Funktion ist vergleichbar der des Landesdatenschutzbeauftragten im staatlichen Bereich. Die Zuständigkeit als Aufsicht über die kirchlichen Einrichtungen beschränkt sich beim Diözesandatenschutzbeauftragten aber auf das Gebiet der (Erz-)Diözese, für die er bestellt wurde.
[2] EuGH Urteil vom 09.03.2010, Rechtssache C-518/07.
[3] EuGH Urteil vom 09.03.2010, Rechtssache C-518/07, Rz. 30.

ist aber die Verpflichtung, dass die derzeit geltenden datenschutzrechtlichen Vorgaben der katholischen Kirche bis Mai 2018, dem Zeitpunkt der Anwendbarkeit der DSGVO, an die Vorgaben der DSGVO angepasst sein müssen. Dies bedeutet eine Neufassung der Anordnung über den Datenschutz – auch hier also Datenschutz 2.0.
Beide Entwicklungen zusammen zeigen deutlich, dass eine Konzentration und fachliche und personelle Stärkung der Datenschutzaufsicht in der katholischen Kirche dringend geboten war.

Die nordrhein-westfälischen (Erz-)Diözesen sind mit dem Schritt der Gründung des Katholischen Datenschutzzentrums als unabhängige Körperschaft des öffentlichen Rechts einen großen Schritt gegangen. Einen großen Schritt hin zu einer unabhängigeren, fachlich breiter aufgestellten Fachbehörde, die die kirchlichen Stellen umfassender in datenschutzrechtlichen und technischen Fragen des Datenschutzes beraten kann und für die Betroffenen eine unabhängige aufsichtsrechtliche Prüfung von Eingaben sicherstellt.

Wir dürfen Sie ermuntern, mit uns diesen eingeschlagenen Weg weiter zu beschreiten – für einen guten Datenschutz in der katholischen Kirche.

„... wurde die Datenschutzaufsicht organisatorisch und personell neu aufgestellt – Datenschutz 2.0 eben."

Steffen Pau
Diözesandatenschutzbeauftragter
und Leiter des Katholischen Datenschutzzentrums

1 Entwicklungen im Datenschutz

1.1 Entwicklungen in der Europäischen Union

Grundlage des derzeit geltenden Bundesdatenschutzgesetzes, das auch die Vorlage für die derzeit gültige Anordnung über den kirchlichen Datenschutz in den katholischen (Erz-)Diözesen bildet, ist die europäische Richtlinie 95/46/EG aus dem Jahr 1995. Zur Reform dieser Richtlinie legte die EU-Kommission Anfang 2012 den Entwurf einer neuen Datenschutzgrundverordnung vor, die das Datenschutzrecht in Europa an die rechtlichen und technischen Entwicklungen seit dem Jahr 1995 anpassen sollte.

Nach über vierjährigen Beratungen verabschiedeten die Gremien der EU die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Ziel der Europäischen Union ist es, ein europaweit einheitlich geltendes Recht zu schaffen und einen möglichst hohen Schutz der personenbezogenen Daten in allen europäischen Mitgliedsstaaten sicherzustellen. Aus diesem Grund ist auch nicht wie bei vorherigen Vorgaben zum Datenschutz auf europäischer Ebene eine Richtlinie erlassen worden, die dann von jedem einzelnen Mitgliedsstaat noch in nationales Recht transformiert werden musste, sondern eine Verordnung, die ohne weiteren nationalen Umsetzungsakt Gültigkeit erlangt.

Schwerpunkte der Regelungen sollten die Sicherstellungen von Informations- und Rechtsansprüchen der Betroffenen bezüglich ihrer personenbezogenen Daten sein, aber auch die Einführung und Absicherung von unabhängigen Datenschutzaufsichten, u.a. zur Beratung, Überwachung und Rechtsdurchsetzung im Bereich des Datenschutzes. Im Rahmen des Gesetzgebungsverfahrens, das schließlich zu einer zwischen EU-Parlament, EU-Rat und EU-Kommission abgestimmten Fassung führte, konnten sich auch die Kirchen im Rahmen des Abstimmungsverfahrens mit der Bundesregierung einbringen. Entscheidende Vorschrift für die Kirchen ist dabei der Art. 91 DSGVO, welcher die Grundlage für den eigenständigen Datenschutz der Kirchen darstellt[4].

Die DSGVO ist am 25. Mai 2016 in Kraft getreten. Um den Anwendern der Verordnung eine geordnete Umsetzung zu ermöglichen, ist die Verordnung erst ab dem 25. Mai 2018 anwendbar.

[4] Nähere Erläuterungen siehe Kapitel 1.3 dieses Berichtes.

1.2 Entwicklungen in der Bundesrepublik Deutschland

„Ab dem 25. Mai 2018 ist die DSGVO anwendbar."

Mit der Anwendbarkeit der DSGVO ab dem 25. Mai 2018 verliert das Bundesdatenschutzgesetz in seiner bisherigen Fassung seine allgemeine Gültigkeit. Daher muss der bundesdeutsche Gesetzgeber die nationalen Datenschutzregelungen an die ab Mai 2018 geltende Rechtslage anpassen. Neben diesen notwendigen Anpassungen der bestehenden Regelungen eröffnet die DSGVO durch Öffnungsklauseln auch Ermächtigungsgrundlagen für den nationalen Gesetzgeber, auf deren Basis in den nationalen Gesetzen Abweichungen und Präzisierungen in Bezug auf die DSGVO geregelt werden können.
Zur Umsetzung dieser Ermächtigungen hat das Innenministerium Ende 2016 einen Referentenentwurf vorgelegt. Dieser Entwurf eines „Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/880 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)"[5] beinhaltet unter anderem die Vorschläge, die sich aus der DSGVO ergebenden Regelungsmöglichkeiten umzusetzen und das nationale Datenschutzrecht in der nötigen Weise anzupassen. Dabei können sich Öffnungen gegenüber der DSGVO und Sonderregelungen in Anbetracht von Besonderheiten in der Bundesrepublik Deutschland ergeben. Der Referentenentwurf soll nach Abschluss des erforderlichen Gesetzgebungsverfahrens zu der Inkraftsetzung eines neugefassten Bundesdatenschutzgesetzes führen.

In dem Entwurf sind zwei aus Sicht des Katholischen Datenschutzzentrums wichtige Regelungen enthalten, die wir hier erwähnen wollen.

Zum einen wird mit dem Gesetzentwurf die Beibehaltung der betrieblichen Datenschutzbeauftragten in dem Umfang vorgesehen, wie er jetzt im geltenden BDSG festgeschrieben ist. Dies ist aus Sicht der Datenschutzaufsicht sehr wichtig zur effektiven Umsetzung und Durchsetzung der datenschutzrechtlichen Regelungen bei den verantwortlichen Stellen, die die Verarbeitung der Daten vornehmen. Die betrieblichen Datenschutzbeauftragten sind als fachlich versierte Ansprechpartner vor Ort die erste Anlaufstelle für Datenschutzfragen der Betriebe und Einrichtungen und für die Beschäftigten sowie die Kunden.

Zum anderen sollen nach der Regelung des § 18 Abs. 1 des Gesetzentwurfes die Datenschutzaufsichtsbehörden der Katholischen (Erz-)Diözesen als Aufsichtsbehörden nach Art 91 DSGVO in die Beratung von Stellungnahmen nach § 18 des Gesetzentwurfes einbezogen werden. Die Datenschutzaufsichten der Kirche können dann eine Stellungnahme abgeben, soweit die Kirche von der betreffenden Frage betroffen ist. Diese Stellungnahme fließt in die Gesamtstellungnahme der Datenschutzbeauftragten des Bundes und der Länder ein.

[5] Mittlerweile als Gesetzesentwurf unter: Bundestags-Drucksache 18/11325 veröffentlicht.

1.3 Entwicklungen in der römisch-katholischen Kirche

Die (Erz-)Diözesen in Deutschland sind selbständige Körperschaften des öffentlichen Rechts. In jeder (Erz-)Diözese hat der jeweilige (Erz-)Bischof die gesetzgebende Gewalt und erlässt eigene Gesetze und Verordnungen für seine (Erz-)Diözese. Die Initiierung eines Gesetzgebungsverfahrens und den Erlass eines Gesetzes durch den (Erz-)Bischof kann dabei auf unabweislichen Regelungsbedürfnissen beruhen, aber auch durch externe Entwicklungen im außerkirchlichen Bereich angestoßen werden. Dazu zählen die Vorgaben auf der Ebene der Europäischen Union und deren zunehmende Bedeutung.
Die DSGVO führt zu der Notwendigkeit für die Kirchen in Deutschland, ihre Datenschutzbestimmung zu ändern und an den Vorgaben der DSGVO auszurichten.
Für die Kirchen enthält die DSGVO eine eigene Regelung in Art. 91 DSGVO. Danach dürfen Kirchen, die zum Zeitpunkt des Inkrafttretens der DSGVO bereits umfassende Regelungen zum Datenschutz erlassen haben, diese weiterhin anwenden, wobei Voraussetzung ist, dass die kirchlichen Regelungen in Einklang mit dieser Verordnung gebracht werden.

Die katholische Kirche in Deutschland hat mit der derzeitigen Anordnung über den kirchlichen Datenschutz Regelungen in dem geforderten Sinne getroffen, die nunmehr in Einklang mit der DSGVO gebracht werden müssen. Art. 91 DSGVO verankert das in Deutschland grundgesetzlich abgesicherte Recht der Kirchen auf Selbstbestimmung. Das in der DSGVO gewährte Recht führt auf der anderen Seite zu der Verpflichtung, von den Möglichkeiten Gebrauch zu machen, insbesondere auch, um nicht der Rechte und Möglichkeiten verlustig zu werden, wenn die gebotenen Spielräume nicht ausgefüllt werden. Daher sind die Kirchen in Deutschland gefordert, den EU-Vorgaben entsprechende Gesetze zu erlassen, wobei diese bis zur Anwendbarkeit der DSGVO ab dem 25. Mai 2018 in Kraft gesetzt sein müssen.

„Daher ist die Kirche gefordert, die KDO vor Mai 2018 zu novellieren."

Zur Schaffung der rechtlichen Grundlagen, die qualitativ und inhaltlich die Vorgaben der Europäischen Union erfüllen, hat der Verband der Diözesen Deutschlands eine Unterarbeitsgruppe der Ständigen Arbeitsgruppe Datenschutz- und Melderecht / IT-Recht der Rechtskommission des VDD zur Novellierung der KDO eingerichtet. Deren Aufgabe ist es, die notwendigen Änderungen der KDO zu beraten und einen Gesetzesvorschlag für die Deutsche Bischofskonferenz bzw. die Vollversammlung der Bischöfe als Gesetzgeber zu entwickeln, der als den Vorgaben des Art. 91 DSGVO entsprechendes Gesetz verabschiedet und in Kraft gesetzt werden kann. Diese Arbeitsgruppe hat ihre Tätigkeit aufgenommen nachdem der Text der DSGVO vorlag und arbeitet intensiv an der Prüfung der erforderlichen Änderungen der bisherigen KDO vor dem Hintergrund der DSGVO und der notwendigen Anpassungen aufgrund der kirchlichen Spezifika und besonderen Strukturen.

In Fortschreibung der Rechtsprechung des Europäischen Gerichtshofes und der bestehenden Regelungen enthält die DSGVO ausführliche Regelungen zu Aufgaben und Befugnissen der Datenschutzaufsichtsbehörden und deren Abstimmung untereinander auf europäischer Ebene.
Der schon erwähnte Art 91 DSGVO legt in seinem Abs. 2 fest, dass Kirchen, die umfassende Datenschutzregeln anwenden, der Aufsicht durch eine unabhängige Datenschutzbehörde unterliegen müssen, die den Regelungen der DSGVO zu den Datenschutzaufsichtsbehörden folgt.
Hier haben die nordrhein-westfälischen (Erz-)Diözesen mit der Errichtung des Katholischen Datenschutzzentrums bereits die erforderliche unabhängige Stelle geschaffen und für die Erfüllung der zwingenden europäischen Vorgabe gesorgt. Die übrigen (Erz-)Diözesen in Deutschland haben gleichfalls regionale Datenschutzaufsichten eingerichtet bzw. errichten diese derzeit.
Auch das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU und die neuen Regelungen sind von Seiten der Kirche darauf zu überprüfen, ob und in welchem Umfang sie in die Novellierung der KDO einfließen können oder gar müssen. Dies wird durch die bereits erwähnte Arbeitsgruppe übernommen.

1.4 Entwicklungen in der evangelischen Kirche

Seit 2014 hat die Evangelische Kirche Deutschlands eine einheitliche Datenschutzaufsicht für sich und nahezu alle Landeskirchen und die Diakonien. Der Beauftragte für den Datenschutz der EKD ist – in der Rechtsform einer unselbständigen Einrichtung der EKD – als unabhängige und eigenständige Dienststelle organisiert und hat seinen Hauptsitz in Hannover. Zur Unterstützung seiner Arbeit sind vier Regionalbüros gebildet worden – in Hannover für den nördlichen Bereich, Berlin für den östlichen Bereich, Dortmund für den Bereich Mitte-West und Ulm für den südlichen Bereich.
Das Datenschutzgesetz der EKD ist – wie die KDO – an die Regelungen des BDSG angelehnt. Die EKD ist derzeit ebenfalls dabei, die datenschutzrechtlichen Regelungen der EKD an die Vorgaben der DSGVO anzupassen, um ein vergleichbares Schutzniveau zu gewährleisten. Daher hat die EKD für die erforderliche Anpassung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland eine vergleichbare Arbeitsgruppe eingerichtet. Die beiden Arbeitsgruppen auf evangelischer und katholischer Seite informieren sich jeweils über den Stand ihrer Beratungen. An den Sitzungen nimmt jeweils ein Mitglied bei der anderen Konfession teil.

1.5 Entwicklung in der Datensicherheit

1.5.1 Ransomware

Das Jahr 2016 stand unter anderen im Zeichen von Verschlüsselungs-Trojanern, wobei diese Art des Angriffs auch im Jahr 2017 noch aktuell ist. Die Verbreitung erfolgt überwiegend durch den Empfang von infizierten

E-Mail Anhängen, die bekannten Unternehmen ähneln. Startet der Anwender die an die E-Mail angehangene Datei, werden alle in dem Benutzerkontext erreichbaren Dateien verschlüsselt und ein „Lösegeld" gefordert. Existiert kein entsprechendes Zugriffs- und Berechtigungskonzept kann der Schaden immens sein. Hier kann nur ein aktuelles Backup den Schaden geringhalten. Die Zahlung des geforderten Lösegelds gibt auch keine hundertprozentige Garantie für die korrekte Entschlüsselung. Ist daher die Sicherung veraltet oder gar nicht vorhanden, sind die Daten in der Regel unwiderruflich verloren. Durch diese Ereignisse ist das Bewusstsein für eine sinnvolle Backup Strategie wieder in den Fokus gekommen. Das nicht nur Privatnutzer betroffen sind, zeigte die besondere Aufmerksamkeit die die Infektion des Lukas Krankenhauses aus Neuss mit einem Verschlüsselungstrojaner hervorrief.

1.5.2 IoT Geräte (Internet of Things)

Elektronische Geräte, die mit dem Internet verbunden sind, greifen immer tiefer in unseren Lebensalltag ein. IoT-Geräte (Kameras, Lautsprecher etc.) sind in 2016 als ein großes Sicherheitsproblem identifiziert worden. Schlechte Programmierung und mangelnde Sicherheit können diese Geräte in ein perfektes Angriffswerkzeug verwandeln. Wobei nicht die Rechenkapazität das lohnende Ziel ist, sondern die schiere Masse an verwundbaren Einheiten. Sind die Geräte infiziert, werden gezielt DDoS (Distributed Denial of Service) Attacken gegen Ziele im Internet geführt. Dies kann im schlimmsten Fall zur Einstellung der Dienste des Angegriffenen und damit zur Nichterreichbarkeit im Internet führen. Aber auch für den einzelnen Nutzer können mangelnde Vorkehrungen zum Datenschutz Folgen haben. So stehen einige dieser Geräte im Verdacht mehr Daten zu sammeln, als für die Dienstleistung benötigt werden. Bei Verlust der Daten beim Unternehmer kann die Reputation des Einzelnen beschädigt werden. Auch kann durch eine umfassende Datensammlung in vielen Lebensbereichen ein „gläserner Nutzer" entstehen.

1.5.3 Störerhaftung

Bisher ist die Verfügbarkeit von freien WLAN-Angeboten in Deutschland durch die sogenannte Störerhaftung gering. Im Juli 2016 trat eine Änderung des Telemediengesetzes in Kraft um die Störerhaftung aufzuheben. Leider blieb der Gesetzgeber sehr unkonkret bei der Neufassung und eröffnet einen großen Interpretationsspielraum. Der EuGH sieht immer noch den Anschlussinhaber in der Pflicht, den Personenkreis der Nutzer zu limitieren[6]. Das heißt, dass das WLAN nicht ohne Zugangskontrolle genutzt werden darf. Wird dieses nicht eingehalten, können Schadensersatzansprüche bei Nutzung von urheberechtlich geschützten Medien per Filesharing eines beliebigen Nutzers entstehen[7]. Daher ist das Angebot für frei zugängliche Internetzugänge in katholischen Einrichtungen in Hinblick auf die Haftungsfrage immer noch problematisch und im Einzelfall zu prüfen.

„Daher ist das Angebot für frei zugängliche Internetzugänge in katholischen Einrichtungen in Hinblick auf die Haftungsfrage immer noch problematisch und im Einzelfall zu prüfen."

[6] EuGH vom 15.09.2016 Az.: C-484/14

[7] BGH vom 24.11.2016 Az.: I ZR 220/15.

2 Die Datenschutzaufsicht in der katholischen Kirche

2.1 Aufbau / Entwicklung

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.
Vor dem Hintergrund der immer komplexeren Aufgaben der Diözesandatenschutzbeauftragten und der Rechtsprechung des Europäischen Gerichtshofes zur Unabhängigkeit der (staatlichen) Datenschutz-Aufsichtsbehörden haben die (Erz-)Diözesen die Initiative ergriffen und bündeln die Aufgaben der Diözesandatenschutzbeauftragten regional.
So haben die bayerischen (Erz-)Diözesen und die norddeutschen (Erz-)Diözesen schon vor 2016 jeweils gemeinsame Diözesandatenschutzbeauftragte bestellt. Zum Jahresbeginn 2016 hat auch der gemeinsame Diözesandatenschutzbeauftragte der ostdeutschen (Erz-)Diözesen seine Arbeit aufgenommen.
Für die (Erz-)Diözesen in Baden-Württemberg, Hessen, Rheinland-Pfalz und dem Saarland wird im Jahr 2017 eine gemeinsame Datenschutzaufsicht in Frankfurt mit einem gemeinsamen Diözesandatenschutzbeauftragten die Arbeit aufnehmen.
Zusammen mit dem Katholischen Datenschutzzentrum werden damit zukünftig fünf Stellen die Datenschutzaufsicht für die (Erz-)Diözesen in Deutschland wahrnehmen. Hinzu kommen noch zwei Beauftragte für die Aufsicht über die Orden päpstlichen Rechts, die von der Deutschen Ordensobernkonferenz bestellt worden sind.

2.2 Konferenz der Diözesandatenschutzbeauftragten

Die Diözesandatenschutzbeauftragten tauschen sich regelmäßig aus. Die Konferenz der Diözesandatenschutzbeauftragten gibt diesem Austausch einen Rahmen.
Neben den Diözesandatenschutzbeauftragten werden zu den Konferenzen auch die beiden von der Deutschen Ordensobernkonferenz bestellten Ordensdatenschutzbeauftragten für die päpstlichen Orden eingeladen. Beratend nehmen noch weitere Vertreter (z.B. des Katholischen Büros in Berlin, des Verbandes der Diözesen Deutschlands oder der Deutschen Ordensobernkonferenz) an den Tagungen teil.

„Die Beratungen dienen dazu, gemeinsame Standpunkte zu verabschieden und gemeinsame Vorgehensweisen zu Themen zu finden.“

Die Beratungen dienen dazu, gemeinsame Standpunkte zu verabschieden und gemeinsame Vorgehensweisen zu Themen zu finden. Ziel ist die einheitliche Auslegung der KDO in allen deutschen (Erz-)Diözesen.
Im Berichtszeitraum fand eine zweitägige Konferenz im Oktober in Magdeburg auf Einladung des Diözesandatenschutzbeauftragten für die ostdeutschen (Erz-)Diözesen statt. Neben der Beratung verschiedenster Themenbereiche wurden auch zwei Beschlüsse zu den betrieblichen Datenschutzbeauftragten gemäß § 20 KDO und zur Veröffentlichung von Ehe- und Altersjubiläen gefasst[8].
Zwischen den Tagungen tauschen sich die Diözesandatenschutzbeauftragten auch in regelmäßigen Videokonferenzen über aktuelle Fragen aus.

[8] Siehe Kapitel 6 dieses Berichtes.

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 beschrieben. Wer der Ansicht ist, dass bei der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch eine (katholische) kirchliche Stelle datenschutzrechtliche Regelungen verletzt worden sind, kann sich gemäß § 15 KDO an den Diözesandatenschutzbeauftragten wenden. Dieser prüft den Sachverhalt und hört dazu die betroffene kirchliche Stelle an, soweit ein Verstoß gegen datenschutzrechtliche Regelungen vorliegt. Wichtig ist dabei das Benachteiligungsverbot des § 15 Abs. 3 KDO: „Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an den Diözesandatenschutzbeauftragten gewendet hat.“ Wer sich an Diözesandatenschutzbeauftragten wendet, darf daher keine Nachteile erleiden.

> **„Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an den Diözesandatenschutzbeauftragten gewendet hat.“**

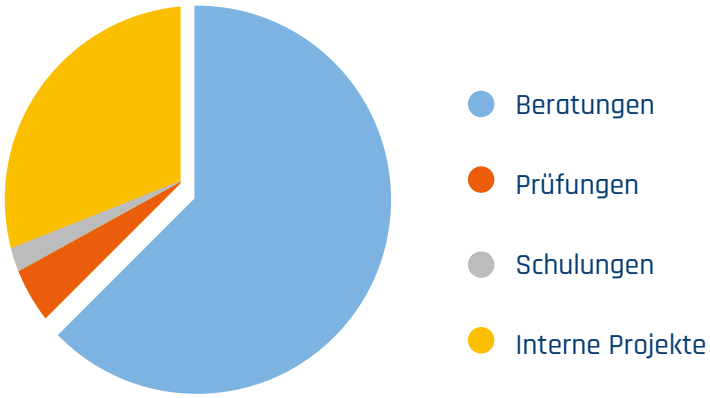
Außer der Bearbeitung von Beschwerden oder Anfragen wacht der Diözesandatenschutzbeauftragte gemäß § 18 Abs. 1 KDO allgemein über die Einhaltung der datenschutzrechtlichen Regelungen. Hierzu führt er anlassbezogen, auf Grund der bei ihm eingehenden Beschwerden, oder ohne Anlass im Rahmen regelmäßiger 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). Datenschutzrecht und Datensicherheit sind beide zwingend notwendig und beide einzuhalten, um Datenschutz sicherzustellen.
Auf Grund des kurzen Zeitraumes wurde in 2016 lediglich eine Anlassprüfung vorgenommen. Auslöser dieser Prüfung war eine Anfrage aus der Einrichtung heraus, die nach weiteren Gesprächen mit allen Beteiligten zu der Prüfung führte. Zu der Anzahl der anlassbezogenen Prüfungen im Jahr 2017 lässt sich noch keine Aussage treffen. Dies ist abhängig von den an das Katholische Datenschutzzentrum herangetragenen Anfragen und Beschwerden und deren Schwere oder Kritikalität.

Für die anlasslosen, regelmäßigen Kontrollen ist für das Jahr 2017 ein Prüfplan erstellt worden, der eine breite Palette an verschiedenen Einrichtungen abdeckt und alle (Erz-)Diözesen im Zuständigkeitsbereich des Katholischen Datenschutzzentrums gleichermaßen berücksichtigt.

Neben der Bearbeitung von Eingaben und der Überwachung der Einhaltung des Datenschutzes berät das Katholische Datenschutzzentrum die kirchlichen Stellen in allen datenschutzrechtlichen Fragestellungen (vgl. § 18 Abs. 1 Satz 3 KDO). Gegenstand einer solchen Beratung können sowohl konkrete Einzelfragen wie z. B. die datenschutzgerechte Durchführung einer Veranstaltung wie auch allgemeine Fragen wie die datenschutzgerechte Gestaltung eines immer wiederkehrenden Prozesses (z. B. Patientenaufnahme im Krankenhaus) sein.
Stellt der Diözesandatenschutzbeauftragte Verstöße gegen datenschutzrechtliche Regelungen fest, kann er diese Verstöße nach § 19 KDO beanstanden und Maßnahmen zur Beseitigung der Verstöße vorgeben. Über die Umsetzung des Maßnahmenplans ist regelmäßig zu berichten; eine Nachprüfung zur Kontrolle der Umsetzung ist möglich.
Damit Verstöße gegen die datenschutzrechtlichen Regelungen möglichst erst gar nicht entstehen, stehen die Kolleginnen und Kollegen des Katholischen Datenschutzzentrums für Vorträge und Fragen zur Verfügung. In den ersten Monaten des Katholischen Datenschutzzentrums sind bereits eine Vielzahl an Anfragen zu Schulungen für den Datenschutz eingegangen. Neben konkreten Anfragen zur Vorstellung des Katholischen Datenschutzzentrums in den unterschiedlichen Gremien und Verbänden ist auch ein großer Bedarf nach Schulungen rund um allgemeine Fragen des Datenschutzes angemeldet worden. In 2017 wird das Katholische Datenschutzzentrum Schulungen für verschiedene Zielgruppen und zu diversen Themen anbieten. Ein Schwerpunkt wird dabei im zweiten Halbjahr 2017 und im ersten Halbjahr 2018 auf Informationsangeboten zur überarbeiteten KDO liegen. Bei Gesprächen in Einrichtungen und Gremien wird kontinuierlich der Bedarf erfragt und die Dienstleistung „Schulung“ von Seiten des Katholischen Datenschutzzentrums angeboten. Die Erkenntnisse aus den Prüfungen und Anfragen fließen ebenfalls in die Schulungen ein.

In den vier Monaten der Tätigkeit des Katholischen Datenschutzzentrums in 2016 waren gut 90 externe Vorgänge zu bearbeiten. Davon waren ca. 70 Prozent der Vorgänge Beratungen, ca. 30 Prozent der Vorgänge Beschwerden, Prüfungen und allgemeine Anfragen. Der hohe Anteil der Beratungsvorgänge zeigt deutlich, dass es einen hohen Beratungsbedarf rund um den Datenschutz in den kirchlichen Einrichtungen gibt. Um diesem Beratungsbedarf gerecht zu werden, wird das Katholische Datenschutzzentrum 2017 gezielt Informationsveranstaltungen und Schulungen anbieten.

Schwerpunkte der Vorgänge 2016



3.2 Einzelne Themen beleuchtet

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

3.2.1 Videoüberwachung

Das Thema Videoüberwachung wurde in verschiedenen Fallgestaltungen an das KDSZ herangetragen. Die Videoüberwachung in Einrichtungen der Altenpflege war ebenso ein Thema wie die Videoüberwachung kirchlicher Gebäude und insbesondere von Kirchen und der damit zusammenhängenden Frage der Beobachtung der Gläubigen bzw. der Beschäftigten.
In § 5a KDO wird, ebenso wie in § 6b BDSG, die Zulässigkeit optisch-elektronischer Einrichtungen zur Beobachtung von öffentlich zugänglichen Räumen behandelt. Damit sind nicht nur die klassischen Videokameras gemeint, sondern alle Geräte, die zur Bildaufzeichnung und Überwachung geeignet sind. Der Begriff Beobachtung meint ferner auch, dass nicht nur die Aufzeichnung von Bildern zu berücksichtigen ist, sondern allein schon die Übertragung auf einen Bildschirm, der von Personen eingesehen werden kann.

„Die Zulässigkeit von Videoüberwachung ist in jedem Einzelfall zu prüfen."

§ 5a KDO beschreibt die Zulässigkeit einer Beobachtung öffentlich zugänglicher Räume. Öffentlich zugängliche Räume sind Räume, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten oder genutzt werden können, d.h. allgemein zugängliche Räume, wie Kirchen, Cafés, öffentliche Parkanlagen, aber auch Eingangsbereiche von Krankenhäusern etc.

Gemäß § 5a Abs. 1 Nr. 1 KDO ist 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 dient. Die Zulässigkeit ist aber in beiden Varianten dann nicht gegeben, wenn bei einer Interessenabwägung die Interessen des Betroffenen überwiegen.

So ist im Einzelfall auf der Grundlage der dokumentierten Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung der Daten über die Zulässigkeit der Videoüberwachung zu entscheiden. Dabei wird z.B. die theoretische Möglichkeit der Begehung einer Straftat und die damit verbundene Hoffnung, diese mittels der Videoüberwachung aufklären zu können, je nach Umfeld der Videoüberwachung im Regelfall nicht ausreichen. Anders kann die Beurteilung ausfallen, wenn schon konkrete Taten begangen wurden oder konkrete Hinweise für solche Taten vorliegen. Ebenso ist die Intensität des Eingriffs zu beurteilen. Welche Räume werden mit welcher Intensität beobachtet? Wird über die Videoüberwachung der Tagesablauf der Beschäftigten oder der Nutzer der kirchlichen Einrichtung lückenlos nachvollziehbar? In Kirchen kommt die Frage hinzu, ob der Kernbereich der Glaubensausübung (z.B. Beichte, Feier der hl. Messe, Gebet) für den Gläubigen unbeobachtet möglich ist.
Sofern eine Beobachtung mit optisch-elektronischen Einrichtungen auch Mitarbeiter erfassen kann, ist eine Beteiligung der Mitarbeitervertretung zu prüfen. Ebenso ist vor Inbetriebnahme zu prüfen, ob die konkrete Anlage zur Videoüberwachung nicht der Vorabkontrolle nach § 3 Abs. 5 KDO unterliegt. Dabei ist insbesondere auf die Risiken für die Rechte und Freiheiten der betroffenen Personen zu achten.

Die Speicherung der aufgezeichneten Daten ist gemäß § 5a Abs. 5 KDO nur solange zulässig, wie sie zur Erreichung des ursprünglichen Zwecks erforderlich sind. Die Daten sind auch zu löschen, wenn schutzwürdige Interessen des Betroffenen der weiteren Speicherung entgegenstehen.

3.2.2 Unerlaubte Weitergabe von personenbezogenen Daten

Eine unerlaubte Weitergabe von personenbezogenen Daten kann absichtlich oder unabsichtlich erfolgen. Wenn für die Weitergabe der Daten keine Rechtsgrundlage vorliegt – sie eben unerlaubt ist – liegt ein Verstoß gegen datenschutzrechtliche Regelungen vor.

So wurde das Katholische Datenschutzzentrum durch die Beschwerde von einer Petentin darüber informiert, dass ihre Tochter, nach einer Behandlung in der Notfallambulanz eines Krankenhauses, von einem unbekannten und an der Behandlung nicht beteiligten Dritten über eine Social-Media-Plattform kontaktiert wurde. An die Kontaktdaten der Tochter war der Dritte über das noch einzusehende Röntgenbild mit der Angabe der personenbezogenen Daten im Behandlungsraum gelangt, als er nach der Tochter der Petentin behandelt wurde. Der Diözesandatenschutzbeauftragte beanstandete diese Datenweitergabe vom Krankenhaus an den Dritten und forderte das Krankenhaus auf, wirksame Maßnahmen zu ergreifen, damit sich solche Sachverhalte nicht wiederholen können.

Eine unerlaubte Weitergabe von personenbezogenen Daten kann dabei auf vielfältige Weise erfolgen. Neben den Fällen, in denen wie hier eine Einsicht in die Daten am Computer erfolgt, kann dies z.B. auch durch eine

Email an einen falschen Adressaten, nicht datenschutzgerecht entsorgte Papierakten, den Verlust eines unverschlüsselten USB-Sticks oder Laptops oder die Weitergabe von Daten an einen sachlich unzuständigen Kollegen geschehen.
Alle diese Fälle können durch technische und/oder organisatorische Maßnahmen im Vorfeld ohne großen Aufwand verhindert werden.

Hier sind die verantwortlichen Stellen gefordert, ihre Prozesse fortlaufend auf datenschutzrechtliche Optimierungsmöglichkeiten zu prüfen und verbesserte Möglichkeiten der Datensicherheit in die Prozesse einzubauen.

3.2.3 Veröffentlichungen in Pfarr- und Gemeindenachrichten

Bei einem großen Anteil der im vergangenen Jahr eingegangenen Anfragen handelte es sich um Fragen zum Thema Veröffentlichungen im Internet. So möchten z.B. viele Gemeinden ihren Pfarr- oder Gemeindebrief im Internet veröffentlichen. In den Pfarr- oder Gemeindebriefen werden jedoch eine Vielzahl von personenbezogenen Daten veröffentlicht. Für eine solche Veröffentlichung ist die Erfüllung der Voraussetzungen der in den nordrhein-westfälischen (Erz-)Diözesen geltenden Ausführungsrichtlinien für den pfarramtlichen Bereich erforderlich, wobei die Veröffentlichung im Internet immer der Einwilligung des Betroffenen bedarf.

Bei der datenschutzrechtlichen Beurteilung ist dabei nach der Art der Daten und der Art der Veröffentlichung zu unterscheiden.
Während die Bekanntmachung von Name, Vorname und Datum bei kirchlichen Amtshandlungen (z. B. Taufen, Erstkommunion, Firmung, Trauung, Weihen und Exequien) als Aushang oder in den gedruckten Pfarrnachrichten möglich ist, bedarf die Veröffentlichung dieser Daten im Internet der vorherigen Einwilligung des Betroffenen. Besteht ein Sperrvermerk ist eine Veröffentlichung immer unzulässig[9].

Bei der Veröffentlichung von Name, Vorname und Datum besonderer Ereignisse (z.B. Alters- und Ehejubiläen, Geburten, Sterbefälle, Ordens- und Priesterjubiläen) kann der Betroffene vorab der Veröffentlichung in den gedruckten Pfarrnachrichten oder dem Aushang widersprechen. Auf dieses Recht ist jährlich in den Pfarrnachrichten oder per Aushang hinzuweisen. Auch hier ist eine Veröffentlichung im Internet nur mit Einwilligung des Betroffenen möglich. Besteht ein Sperrvermerk ist eine Veröffentlichung immer unzulässig[10].

3.2.4 Cloud-Nutzung

Seit einigen Jahren verstärkt sich die Nutzung von Cloud-Diensten. Cloud beschreibt die Konsolidierung von Rechnerkapazitäten an zentrale

[9] Siehe Abschnitt II Nr. 4 der Ausführungsrichtlinien zur Anordnung über den kirchlichen Datenschutz - KDO - für den pfarramtlichen Bereich der jeweiligen (Erz-)Diözese.
[10] Siehe Abschnitt II Nr. 5 der Ausführungsrichtlinien zur Anordnung über den kirchlichen Datenschutz - KDO - für den pfarramtlichen Bereich der jeweiligen (Erz-)Diözese.

Stellen. Die Vorteile liegen besonders in der Verwaltbarkeit der Computerinstanzen und deren Sicherung. Cloud-Konfigurationen können nicht nur in der eigenen Umgebung (Private Cloud) betrieben, sondern auch bei externen Dienstleistern angemietet werden (Public Cloud). In diesem Fall nutzt der Kunde die Rechnerkapazitäten mit vielen anderen Kunden gemeinsam, durch diese Skalierung werden Preisvorteile erreicht. Cloud-Produkte werden in verschiedene Betriebsmodelle sortiert, die auch den Umfang der Administration bestimmen. „Software as a Service" (SaaS) beinhaltet Produkte, die sofort vom Kunden ohne Installationsaufwand genutzt werden können. Viele Nutzer verwenden bereits solch ein Betriebsmodell, sobald sie z.B. einen externen Anbieter für die E-Mail-Kommunikation nutzen. „Plattform as a Service" (PaaS) bietet eine Grundlage für den Aufbau von Diensten. Der Kunden muss gewisse Konfigurationen und Installationen selbst vornehmen. Den größten Freiheitsgrad erhalten Kunden bei „Infrastructure as a Service" (IaaS), in dem sie den Inhalt der virtuellen Maschinen selbst bestimmen können. Die Daten von unterschiedlichen Kunden werden logisch durch verschiedene Mechanismen separiert.

Aus datenschutzrechtlicher Sicht sind bei den verschiedenen Varianten der Cloud-Nutzung viele Fragen zu beantworten. So ist von der verantwortlichen Stelle, die die Cloud-Dienste nutzen will, zu prüfen, wo die Daten vom Cloud-Dienstleister gespeichert werden.

„Gemäß den einschlägigen Regelungen in der KDO-DVO ist eine Cloud-Nutzung derzeit nur im Geltungsbereich des BDSG möglich."

In diesem Zusammenhang ist auf die Vorschrift der Zf. 4.2 der Anlage 3 in Abschnitt IV. der Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz hinzuweisen, nach der eine Speicherung von Cloud-Daten bis zur Anwendung der DSGVO im Mai 2018 nur im Geltungsbereich des BDSG, also in Deutschland, erlaubt ist.

Außerdem ist zu regeln, wer von welchem Ort der Welt beispielsweise die Wartungszugriffe durchführt. Auch ist sicherzustellen, dass die Daten der verschiedenen Kunden des Cloud-Dienstes gegeneinander sicher getrennt sind. Ebenso spielen Fragen der Verschlüsselung der Daten in der Cloud und auf dem Weg vom Kunden zur Cloud oder allgemein die technisch-organisatorischen Maßnahmen zum Schutz der Daten neben vielen einzelfallspezifischen Fragen eine zentrale Rolle bei der datenschutzrechtlichen Beurteilung der konkreten Cloud-Lösung.

In jedem der Betriebsmodelle muss ein entsprechender Vertrag zur Auftragsdatenverarbeitung nach § 8 KDO[11] eingegangen werden. Wie bei allen Auftragsdatenverarbeitungen hat sich der Auftraggeber auch hier vor Beginn der Verarbeitung von der Einhaltung der vertraglich vereinbarten technisch-organisatorischen Maßnahmen zu überzeugen.

3.2.5 Einwilligungen

In vielen Anfragen an das Katholische Datenschutzzentrum wurde deutlich, dass die Erfordernisse für eine datenschutzrechtliche Einwilligung

[11] Vergleichbar § 11 BDSG.

häufig unklar sind und im Einzelfall nicht erfüllt werden. Die Einwilligung wird in § 3 KDO – analog zu § 4 BDSG – als eine der möglichen Rechtsgrundlagen für die Erhebung, Verarbeitung oder Nutzung von personenbezogen Daten aufgeführt. Über die Form und Gestaltung der Einwilligung wird in § 3 Abs. 2 bis 4 KDO näher eingegangen.

Für die Umsetzung in den kirchlichen Einrichtungen der Diözesen heißt das, dass die verantwortliche Stelle (Einrichtung, Institution, Gemeinde, Jugendgruppe o.ä.) vor der Verarbeitung der Daten das Einverständnis des Betroffenen einholen muss. Erst wenn der Betroffene erklärt hat, dass er mit der Datenverarbeitung einverstanden ist, darf die Erhebung, Verarbeitung oder Nutzung der Daten erfolgen.
Eine wirksame Einwilligung muss freiwillig, schriftlich und informiert erfolgen. Dies bedeutet,

- dass der Person bei der Erklärung des Einverständnisses bewusst sein muss, dass sie ihre Daten nicht mitteilen muss. Die Wirksamkeit hängt dabei nicht von der Geschäftsfähigkeit des Betroffenen, sondern von der Urteils- und Einsichtsfähigkeit ab. Sind jedoch Persönlichkeitsrechte oder wirtschaftliche Interessen betroffen (Bilder oder Videos; Zahlung von Mitgliedsbeiträgen) ist die Einwilligung des Betroffen und (soweit erforderlich) des gesetzlichen Vertreters/Betreuers einzuholen.
- dass die Einwilligung schriftlich zu erklären ist. Ausnahmen sind im Gesetz geregelt (z.B. für Zwecke der wissenschaftlichen Forschung).
- dass die Person, die einwilligt, über Art und Umfang der Einwilligung umfassend informiert sein muss, bevor sie einwilligt. Welche Aufklärungspflichten im Einzelfall bestehen, ergibt sich aus dem jeweiligen Verwendungszweck. 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.

4 Das Katholische Datenschutzzentrum

4.1 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 über sieben Millionen Menschen (Stand 2015) römisch-katholischen Glaubens.

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.

4.2 Aufbau der Einrichtung

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

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

Dem Diözesandatenschutzbeauftragten sind ein Vertreter, Referenten und Sekretariatskräfte zur Seite gestellt, die auch vom KDSZ angestellt

sind. Von den bis zum 31.12.2016 genehmigten acht Stellen sind zum Jahresende sechs besetzt. Eine Stelle wird zum 01.04.2017 besetzt werden können. Eine weitere Stelle ist in der Ausschreibung.

	Soll	Ist
Leitung KDSZ / Diözesandatenschutzbeauftragter	1	1
Stellv. Leitung KDSZ / stellv. Diözesandatenschutzbeauftragter	1	1
Referentinnen / Referenten	4	2
Sekretariat	2	2
Gesamt	**8**	**6**

Personalausstattung KDSZ zum 31.12.2016 (in Vollzeitstellen)

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

Bei der Planung des KDSZ wurde konsequent auf die Umsetzung des Urteils des Europäischen Gerichtshofes vom 09.03.2010[12] zur Unabhängigkeit und Selbständigkeit der Datenschutzaufsichtsbehörden geachtet und die Veränderungen durch die Europäische Datenschutzgrundverordnung bzw. deren Umsetzung in kirchliches Recht schon berücksichtigt.

Das KDSZ hat seinen Sitz im Hause des Sozialinstituts der Kommende Dortmund, einer Einrichtung des Erzbistums Paderborn, gefunden. Neben der Übernahme der Aufgaben des Diözesandatenschutzbeauftragten der fünf (Erz-)Diözesen in NRW zum 01.09.2016 war es in den verbleibenden Monaten des Jahres 2016 auch Ziel, die Organisation des KDSZ aufzubauen. Die vom Erzbistum Paderborn gestellte Räumlichkeiten wurden mit modernen Büroarbeitsplätzen eingerichtet. Dies verlief ebenso reibungslos wie die Personalgewinnung. Für die Unterstützung nochmals einen herzlichen Dank an alle beteiligten Stellen.

Das Katholische Datenschutzzentrum konnte die Startphase in den vier Monaten seit dem Start noch nicht ganz verlassen. So wird der Internetauftritt unter **www.katholisches-datenschutzzentrum.de** erst Ende des ersten Quartals 2017 fertig werden. Auch kann das geplante Informationsmaterial erst nach und nach erstellt und dann zur Verfügung gestellt

[12] EuGH Urteil vom 09.03.2010, Rechtssache C-518/07.

werden. Ebenso wird in Gesprächen mit vielen Stellen noch an den Konzepten für Schulungen gearbeitet. Hier wird noch der Bedarf abgefragt und dann die passenden Lösungen erarbeitet. Die organisatorischen Prozesse sollen weitgehend in 2017 abgeschlossen werden.

Auch ist zu berücksichtigen, dass die DSGVO bzw. die Umsetzung in der neuen KDO auch neue Aufgaben und Anforderungen an die Datenschutzaufsicht mit sich bringt, die beim weiteren Aufbau des Datenschutzzentrums direkt mit umzusetzen sind.

4.3 Finanzen

Das KDSZ wird von den fünf (Erz-)Diözesen als Mitgliedern 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 Rumpfjahr 2016, in dem das KDSZ nur von der Aufnahme der Tätigkeit des gemeinsamen Diözesandatenschutzbeauftragten im September bis Dezember zu finanzieren war, haben die fünf Mitgliedsdiözesen einen pauschalen Betrag zur Verfügung gestellt, mit dem die notwendigen Kosten der Ersteinrichtung für Büro und Informationstechnik, der Personalgewinnung, der Personalkosten und des laufenden Geschäfts gedeckt waren.

Für das Jahr 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.

4.4 Vertretung in Gremien und Arbeitsgruppen in der katholischen Kirche

Derzeit wird in einer Unterarbeitsgruppe der Ständigen Arbeitsgruppe Datenschutz- und Melderecht/IT-Recht der Rechtskommission des VDD ein Vorschlag für die Neufassung der KDO erarbeitet. Diese Neufassung ist auf Grund der DSGVO notwendig. Ein Referent des KDSZ trägt als Mitglied dieser Unterarbeitsgruppe zur Entwicklung der neuen Datenschutzregeln der Katholischen Kirche in Deutschland bei.
Bei der Weiterentwicklung der diözesanen Gesetze und der Diskussion von grundsätzlichen Rechtsfragen sind die Justitiarinnen und Justitiare der fünf (Erz-)Diözesen die ersten Ansprechpartner des Katholischen Datenschutzzentrums. Zum besseren Austausch haben die Justitiarskonferenz NRW und das KDSZ besprochen, dass der Diözesandatenschutzbeauftragte themenbezogen zu den Sitzungen der Justitiarinnen und Justitiare hinzukommt und damit ein regelmäßiger Austausch auf dieser Ebene sichergestellt ist.

4.5 Vernetzung

4.5.1 Vernetzung mit kirchlichen Stellen

Die Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen stehen in ständigem Austausch zu aktuellen Fragen und grundsätzlichen Themen. Die Besprechungen oder Videokonferenzen dienen diesem Austausch und der Vorbereitung und Verabschiedung gemeinsamer Beschlüsse[13].
Der Beauftragte für den Datenschutz in der EKD (BfD EKD) hat neben seinem Hauptsitz in Hannover noch vier Außenstellen. Die Außenstelle in Dortmund ist u.a. für die Landeskirchen in NRW zuständig.
Der Diözesandatenschutzbeauftragte und sein Vertreter haben sich zu einem ersten Austausch mit dem Regionalverantwortlichen des Dortmunder Büros des BfD EKD getroffen. Dieser Austausch soll fortgesetzt werden und themenbezogen auch intensiviert werden. Ein Treffen mit dem BfD EKD ist für das erste Quartal 2017 geplant.

4.5.2 Vernetzung mit staatlichen Stellen

Der Kontakt und der Austausch mit der Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten als staatlichen Datenschutzaufsichtsbehörden ist nach § 18 Abs. 5 KDO Bestandteil der Aufgaben des Diözesandatenschutzbeauftragten.
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.
Ein erstes persönliches Gespräch zwischen der Landesdatenschutzbeauftragten NRW und dem Diözesandatenschutzbeauftragten diente dem allgemeinen Austausch. Dieser Austausch wird auch auf der Fachebene sach- und themenbezogen fortgesetzt.

4.6 Öffentlichkeitsarbeit

Durch Schulungen und Beratungen vor Ort versucht das KDSZ, das Thema Datenschutz voranzubringen und die Einrichtung KDSZ bekannter zu machen. Dabei soll der Fokus in erster Linie auf der Dienstleistungstätigkeit der Beratung und Unterstützung bei Fragen liegen.
Seit Beginn der Tätigkeit des KDSZ zeigte sich, dass der Informationsbedarf zum Thema Datenschutz sehr hoch war. Um hier einfach Informationen an größere Nutzergruppen zur Verfügung stellen zu können, begann das KDSZ kurz nach dem Start mit der Entwicklung der eigenen Internetpräsenz.

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

Die Internetseiten, die unter **www.katholisches-datenschutzzentrum.de** erreichbar sind, werden gegen Ende des ersten Quartals 2017 fertiggestellt werden.

Neben allgemeinen Informationen sollen verschiedene Handreichungen und ein Newsletter angeboten werden.
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.
Wir würden uns freuen, wenn diese Informationsplattform rege angenommen wird. Anregungen und Themenwünsche zur weiteren Vervollständigung der Internetpräsenz sind jederzeit willkommen.

5 Ausblick

Neben der Bearbeitung aktueller Anfragen und Beschwerden lag der Schwerpunkt der Arbeit des KDSZ in den vier Monaten 2016 im Aufbau der Einrichtung. Organisatorische Fragen standen im Vordergrund.

In 2017 werden diese dem Aufbau der neuen Einrichtung geschuldeten organisatorischen Fragen mehr und mehr zurücktreten und die inhaltliche Arbeit den Schwerpunkt bilden.
Hierbei wird neben der Bearbeitung der schon in den ersten Wochen zahlreichen Anfragen und Beschwerden der Ausbau des Beratungsangebotes ein Schwerpunkt sein.

Ende des ersten Quartals 2017 ist die Inbetriebnahme des Internetauftritts des KDSZ geplant. Der Ausbau des Informationsangebotes im Internet wird auch in den folgenden Monaten ein Schwerpunkt sein.
Neben den anlassbezogenen Prüfungen werden in 2017 vermehrt kirchliche Einrichtungen der fünf (Erz-)Diözesen in Regelprüfungen (also ohne konkreten Anlass einer Beschwerde o.ä.) geprüft werden. Aber auch dabei soll der beratende Aspekt im Vordergrund stehen. So soll die Akzeptanz zur Umsetzung der Vorgaben des kirchlichen Datenschutzes gefördert werden.

Auch wird das KDSZ in 2017 mit Verfahrens-/Prozessaufnahmen in den zentralen Einheiten der fünf (Erz-)Diözesen beginnen. Den Start wird das KDSZ mit Verfahrensaufnahmen in den fünf Generalvikariaten machen. Ziel dieser Verfahrensaufnahmen ist es, einen besseren Einblick in die Arbeit und den Umgang mit personenbezogenen Daten in den Diözesen zu bekommen.

Einen Schwerpunkt im zweiten Halbjahr 2017 werden Schulungen bilden. Hier ist vor allem an die Vermittlung der neuen Grundlagen im kirchlichen Datenschutz gedacht, wie sie durch die derzeit noch zu erarbeitende Neufassung der KDO vorgegeben werden.
Bei der Organisation und Durchführung will das Katholische Datenschutzzentrum auf bereits bestehende Fort- und Weiterbildungsangebote der (Erz-)Diözesen zurückgreifen. So soll ein flächendeckendes Angebot in ganz Nordrhein-Westfalen angeboten werden.

Darüber hinaus soll ein fester Schulungskalender etabliert werden. Dabei sollen Erfahrungsaustausche für betriebliche Datenschutzbeauftragte und Einführungsveranstaltungen zum Datenschutz in der Katholischen Kirche und zielgruppenorientierte Angebote für kirchliche Einrichtungen angeboten werden.

Im Jahr 2017 wird die bereits erwähnte Unterarbeitsgruppe zur Novellierung der KDO ihre Arbeit fortsetzen, um einen den Vorgaben der DSGVO entsprechenden Gesetzesentwurf zu erarbeiten. Vor der Vorlage einer endgültigen Fassung sind Anhörungen der (Erz-)Diözesen, der Diözesanjuristen und der Diözesandatenschutzbeauftragten geplant sowie die

„Einen Schwerpunkt im zweiten Halbjahr 2017 werden Schulungen bilden. Hier ist vor allem an die Vermittlung der neuen Grundlagen im kirchlichen Datenschutz gedacht …“

Einbeziehung der im Gesetzgebungsverfahren zu beteiligenden Gremien und Kommissionen.

Für das Jahr 2017 stehen damit viele interessante Aufgabe und Themen an. Wir freuen uns auf eine konstruktive und kooperative Zusammenarbeit mit den Einrichtungen und Institutionen.

6 Anhang – Entschließungen der Konferenz der Diözesandaten-schutzbeauftragten

6.1 Betrieblicher Datenschutzbeauftragter gem. § 20 KDO

[Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 19.-20. November 2016]

Einführung

Die Aufgabe des betrieblichen Datenschutzbeauftragten ist mit der Novellierung der KDO im Jahr 2006 unter dem § 18a eingeführt worden.
Kirchliche Stellen konnten nach dieser Vorschrift einen Datenschutzbeauftragten bestellen.
Mit der Neufassung der KDO im Jahr 2014 finden sich die Vorschriften über den betrieblichen Datenschutzbeauftragten in den §§ 20f. Die Bestellung ist nunmehr differenzierter geregelt. Zwar entspricht § 20 Abs. 1 noch immer dem Wortlaut des alten § 18a, jedoch wurde diese Regelung durch den Abs. 2 ergänzt, nachdem ein betrieblicher Datenschutzbeauftragter bestellt werden soll, wenn mit der automatisierten Datenerhebung, -verarbeitung oder -nutzung mehr als zehn Personen befasst sind.

1. Ermessensausübung

Die Rechtsbegriffe „kann", „sollen" und „müssen" regeln das Ermessen der verpflichteten Stelle. Während der Begriff „kann" die jeweils verantwortliche Stelle lediglich zur Ausübung pflichtgemäßen Ermessens verpflichtet, räumt der Begriff „muss" kein Ermessen ein.[14]
Bei einer „Soll"-Vorschrift ist die verantwortliche Stelle im Regelfall zum Tätigwerden strikt verpflichtet. Wenn sie es nicht macht, muss sie nachweisen, dass ein atypischer Fall vorliegt. Es müssen konkrete, nicht von der zuständigen Stelle selbst zu vertretende Gründe für das Abweichen von der Norm sprechen.[15] Um von einem atypischen Fall sprechen zu können, muss die Abweichung so bedeutend sein, dass das Geweicht der für die Regelentscheidung maßgeblichen Gründe beseitigt wird.[16] Da jeder Ortsbischof die KDO in seinem Bistum als eigenes Recht übernehmen muss, ist nicht davon auszugehen, dass eine Rechtsvorschrift eingeführt wird, deren Umsetzung den verpflichteten Stellen im Bistum nicht möglich ist. Aus diesem Grunde wird die Regelung des § 20 Abs. 2 trotz der Formulierung „soll" als eine „Muss-Vorschrift" betrachtet werden müssen.

2. personenbezogene Daten

Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmbaren oder bestimmten natürlichen Person (§ 2 Abs. 1 KDO)

[14] Bader/Ronellenfitsch Kommentar zum VwVfG 2010, § 40 Rn. 35.

[15] Kopp/Ramsauer Kommentar zum VwVfG 16. Auflage 2015, § 40 Rn. 63.

[16] Sachs in Stelkens/Bonk/Sachs Kommentar zum VwVfG 8. Auflage 2014 § 40 Rn. 27.

3. Automatisiertes Verfahren
Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz einer Datenverarbeitungsanlage. (§ 2 Abs. 2 KDO).

4. Anzahl der Personen
Die Formulierung „Personen" ist wörtlich zu verstehen. Auf das der Datenerhebung, -verarbeitung oder –nutzung zugrundeliegende Rechtsverhältnis kommt es deshalb nicht an. Deshalb ist eine Arbeitnehmereigenschaft im Sinne einer arbeitsvertraglichen Bindung an die verantwortliche Stelle nicht erforderlich. Leiharbeitnehmer, freie Mitarbeiter, Praktikanten und Auszubildende sind deshalb in die Anzahl mit einzubeziehen. So auch die Durchführungsverordnung zur KDO zu § 4 KDO: Zum Kreis der bei der Datenverarbeitung tätigen Personen ... gehören die in den Stellen gem. § 1 Abs. 2 KDO gegen Entgelt beschäftigten und ehrenamtlich tätigen Personen.[17]
Jede Person ist unabhängig vom Umfang ihrer Tätigkeit als eine Person zu zählen. Eine unterschiedliche Berechnung nach dem Umfang des Beschäftigungsverhältnisses, wie sie das Kündigungsschutzgesetz kennt, ist nicht vorzunehmen. Ebenso ist unerheblich, welchen Anteil der Arbeitszeit die Person mit der Datenverarbeitung verbringt.

Entgegen der Parallelvorschrift des BDSG sieht die KDO keine „regelmäßige" Beschäftigung von mehr als zehn Personen vor, sondern formuliert absolut (sind ... befasst). Gleichwohl ist auch hier davon auszugehen, dass temporäre Schwankungen nicht dazu führen, dass die Verpflichtung einen betrieblichen Datenschutzbeauftragten zu bestellen, entfällt oder ein bereits bestellter betrieblicher Datenschutzbeauftragter seine Verpflichtung verliert, weil die Zahl der Personen vorübergehend unter elf sinkt.[18]

5. Zuordnung
Kirchliche Stellen im Sinne des § 1 Abs. 2 KDO sind solche, die eine eigene Rechtspersönlichkeit besitzen. Rechtlich unselbständige Einrichtungen benötigen keinen eigenen betrieblichen Datenschutzbeauftragten, sondern gehören in den Zuständigkeitsbereich des betrieblichen Datenschutzbeauftragten der rechtlich selbständigen Einheit. In organisatorischer Hinsicht erscheint es sinnvoll, dem zuständigen Datenschutzbeauftragten in einem solchen Fall „Hilfskräfte" für die einzelnen unselbständigen Einheiten an die Seite zu stellen. Für diese „Hilfskräfte" gelten dann aber nicht die Regelungen für den betrieblichen Datenschutzbeauftragten. Insbesondere genießen diese nicht den Kündigungsschutz des § 20 Abs. 6 KDO. Soweit Kirchlichen Stellen im Sinne des § 1 Abs. 2 KDO mehrere selbständige Einheiten angehören, ist jede von ihnen verpflichtet, einen eigenen betrieblichen Datenschutzbeauftragten zu bestellen. (So macht es einen Unterschied, ob die Schulen eines Bistums einer selbständigen Stiftung angehören, dann ist für diese Stiftung ein betrieblicher Datenschutzbeauftragter zu bestellen, oder ob die Schulen unselbständige Einrichtungen

[17] KDO-DVO i.d.F. des Beschlusses der Rechtskommission vom 19.03.2015, II. Zu § 4 KDO.
[18] Zum BDSG Simitis § 4f Rn. 19.

sind, die von einer Abteilung des betreffenden Ordinariates/Generalvikariates verwaltet werden. Für letztere ist der betriebliche Datenschutzbeauftragte dieses Generalvikariates verantwortlich.[19])

6. Wahlfreiheit

In § 20 Abs. 3 S. 2 räumt die KDO der verantwortlichen Stelle die Wahlmöglichkeit zwischen einem internen und einem externen betrieblichen Datenschutzbeauftragten ein. Nach der Ordnung sind beide Möglichkeiten gleichrangig, so dass es allein eine Entscheidung der verantwortlichen Stelle ist, für welche Möglichkeit sie sich entscheidet.
Hat sich die verantwortliche Stelle jedoch eine der beiden Möglichkeiten entschieden, so kann sie diese Entscheidung bis zum Ablauf der Frist für die die Entscheidung getroffen worden ist nicht widerrufen. Die Zulassung einer jederzeitigen Widerrufsmöglichkeit aufgrund einer organisatorischen Neuentscheidung und die Anerkennung einer freien Strukturentscheidung als wichtiger Grund würden dazu führen, dass der besondere Abberufungsschutz zur Disposition der verantwortlichen Stelle führt.[20]

7. Natürliche oder juristische Person

Die KDO legt mit dieser Formulierung ebenso wie die Parallelvorschrift des BDSG nahe, dass es sich um eine natürliche Person handeln müsse. Tatsächlich wird dies auch vertreten.[21] Eine ausdrückliche Festlegung durch die KDO auf natürliche Personen besteht aber nicht, deshalb ist der Gegenauffassung der Vorrang einzuräumen, die auch eine Übertragung dieser Aufgabe an juristische Personen für möglich hält[22]. Insbesondere greift die Argumentation nicht, dass nur eine natürliche Person über die geforderte Fachkunde und Zuverlässigkeit verfügen können[23]. Gegenüber der verantwortlichen Stelle ist die juristische Person Ansprechpartner, die aus ihrem Kreis einen kompetenten Bearbeiter auswählt. Im Rahmen zunehmender Komplexität der datenschutzrechtlichen Fragestellungen dürfte das kein Negativkriterium sein.
Unabhängig davon, ob der betriebliche Datenschutzbeauftragte ein interner oder externer ist, handelt es sich bei dieser Person nicht um einen „Dritten“ i. S. von § 2 Abs. 9 S. 2 KDO.

8. Fachkunde und Zuverlässigkeit

Die KDO fordert Fachkunde und Zuverlässigkeit für die Bestellung zum betrieblichen Datenschutzbeauftragten. Insoweit sind rechtliche, organisatorische und technische Kenntnisse gefordert, ohne dass es ein bestimmtes Anforderungsprofil gibt[24], oder ein umfassendes Allround-Wissen gefordert werden könnte[25]. Die geforderte Fachkunde darf insofern nicht mit der Forderung nach ausgeprägtem Spezialwissen in rechtlichem,

---

19 Zur Parallelvorschrift des BDSG Simitis § 4 f Rn. 39.

20 BAG vom 23.03.2011 – 10 AZR 562/09; NZA 2011, 1036, 1037.

21 Däubler in DKWW § 4f Rn. 22; Schierbaum AiB 2001, 514; ders. PersR 2011, 454, 455.

22 Simitis, § 4f Rn. 48.

23 Bergmann/Möhrle/Herb § 4f Rn. 93.

24 Simitis, § 4f Rn. 84.

25 Däubler DKWW § 4f Rn. 28.

organisatorischem oder technischem Bereich gleichgesetzt werden.[26]
Fachkunde bedeutet zunächst, dass der Datenschutzbeauftragte die gesetzlichen Regelungen kennt und sicher anwenden kann.[27] Richtungsweisend für die Anforderungen an die Fachkunde sind die vom Düsseldorfer Kreis am 24./25. November 2010 beschlossenen Mindestanforderungen.[28]

Der Begriff der Zuverlässigkeit umfasst zum einen sorgfältige und gründliche Arbeitsweise, Belastbarkeit, Lernfähigkeit, Loyalität und Gewissenhaftigkeit. Zum anderen darf es keine Interessenskonflikte der Aufgabe des betrieblichen Datenschutzbeauftragten mit anderen hauptamtlichen Aufgaben des Datenschutzbeauftragten geben.[29]
Im Rahmen der Zuverlässigkeit ist insbesondere zu prüfen, ob Interessenkollisionen der Bestellung zum betrieblichen Datenschutzbeauftragten entgegenstehen können. Hierbei setzt eine verlässliche Kontrolle eine klare Trennung zwischen dem betrieblichen Datenschutzbeauftragten und der verantwortlichen Stelle voraus.[30]

8.1.
Fraglich im kirchlichen Bereich erscheint es, ob Mitglieder eines Ordinariatsrates als betriebliche Datenschutzbeauftragte bestellt werden können oder ob dem die Nähe zur Leitung der verantwortlichen Stelle entgegensteht. Für den staatlichen Bereich wird dies für leitende Mitarbeiter in der Literatur uneinheitlich beantwortet. Die bloße Zugehörigkeit zu dieser Gruppe allein soll noch keinen Hinderungsgrund darstellen.[31] Vielmehr soll es auf die weitere Tätigkeit ankommen und darauf, ob diese mit der Verarbeitung personenbezogener Daten zusammenhängen oder darauf Einfluss haben.[32] Dies wird in Ordinariatsräten regelmäßig der Fall sein, da in diesen Gremien „die Fäden zusammenlaufen", in dem Sinne, dass dort Personal- Rechts- Finanzfragen besprochen werden.
Im Falle des Ordinariatsrates ist darüber hinaus zu beachten, dass mit der Mitgliedschaft in diesem Gremium regelmäßig die als Titel geführte Bezeichnung „Ordinariatsrat" / „Ordinariatsrätin" von den Mitgliedern geführt wird. Dieser Titel genießt im kirchlichen Wirkungskreis Anerkennung und zeichnet den Träger aus. Gleichwohl gibt es regelmäßig keine Titelordnung, die einen Anspruch auf diesen Titel gewährt. Auch die bloße Mitgliedschaft in dem Gremium führt nicht in allen Bistümern dazu, dass dessen Mitglieder den persönlichen Titel „Ordinariatsrat" /Ordinariatsrätin" führen dürfen.

---

[26] Simitis § 4f Rn. 93; zu weit gehend insofern der sog. „Ulmer Beschluss" LG Ulm, 5 T 152/90-01 wenn gefordert wird, dass es sich bei dem betrieblichen Datenschutzbeauftragten um einen „Computerexperten" handeln muss.

[27] Bundesbeauftragte für Datenschutz und Informationsfreiheit, Info 4 .
„Die Datenschutzbeauftragten in Behörden und Betrieb", S. 12.

[28] Abgedruckt u. a. in Bundesbeauftragte für Datenschutz und Informationsfreiheit, Info 4
„Die Datenschutzbeauftragten in Behörden und Betrieb", Anhang 9.

[29] Der betriebliche Beauftragte für den Datenschutz des Landes Baden- Württemberg Handreichung für die Bestellung zum betrieblichen Datenschutzbeauftragten - Stand: 17. Juni 2014 -, S. 5.

[30] BAG 22.03.1994 – 1 ABR 51/93, DB 1994, 1678.

[31] Bergmann/Möhrle/Herb § 4f Rn. 109; Simitis § 4f Rn. 99; a. A. "höchst fraglich" Tinnefeld CR 1991, 29, 32; "ungeeignet" Däubler DKWW § 4f Rn. 31.

[32] Simitis § 4f Rn. 99.

Dieser persönliche Titel wird durch den jeweiligen Bischof verliehen oder entzogen. Wenn mit dem persönlichen Titel jedoch ein Status nach außen verbunden ist und der Titelträger sich dessen bewusst ist, dass ihm der Titel jederzeit entzogen werden kann, wird er kaum geneigt sein eine kritische Distanz gegenüber der Bistumsleitung an den Tag zu legen, die ggf. im Sinne des Datenschutzes erforderlich ist.
Eine Beauftragung eines Mitgliedes des Ordinariatsrates ist mithin abzulehnen.

8.2.
Die Bestellung eines Justitiars zum Datenschutzbeauftragten ist für das staatliche Recht umstritten. Das tragende Argument der Gegner ist dabei die Behauptung, dass das Datenschutzrecht von zahlreichen unbestimmten Rechtsbegriffen geprägt ist und so einen weiten Auslegungsspielraum eröffnet, der von Justitiaren regelmäßig im Interesse der verantwortlichen Stelle und „eines reibungslosen Arbeitsablaufs“[33] interpretiert werden[34]. Eine derartige Unterstellung erscheint nicht schlüssig, insbesondere ist nicht nachvollziehbar, warum diese nicht für andere Mitarbeiter in gleicher Weise gelten sollte. Ein Justitiar, wie auch ein beratender Rechtsanwalt ist ständig damit konfrontiert, etwaige Interessenkollisionen aufzulösen und wird seinem Arbeitgeber bzw. seinem Mandanten regelmäßig eine rechtskonforme Lösung vorschlagen. Eine Interessenwahrung für die verantwortliche Stelle steht regelmäßig überhaupt nicht in Widerspruch zur Gewährleistung des gesetzlichen Standards im Datenschutz.[35] Problematisch werden kann die Doppelfunktion allerdings dann, wenn der Datenschutzbeauftragte und Justitiar in Gerichtsprozessen gegen Mitarbeiter oder in Disziplinarverfahren tätig wird.[36]

8.3.
Die für die EDV-Abteilung verantwortliche Person, sowie der/die Leiter/in des Meldewesens kann nicht zum nebenberuflichen betrieblichen Datenschutzbeauftragten bestellt werden.[37] Dies ist nachvollziehbar, da die betreffenden Personen sich selbst kontrollieren müssten. Dies ließe sich mit organisatorischen Maßnahmen nicht ausgleichen und führte dazu, dass der Leiter der EDV bzw. des Meldewesens Ansprüchen ausgesetzt wäre, die einander widersprechen.

8.4.
Leiter und Mitglieder der Personalabteilungen können nach h. M. in Literatur und den Hinweisen der Landesdatenschutzbeauftragten sowie der Bundesbeauftragten für Datenschutz und Informationsfreiheit nicht zum betrieblichen Datenschutzbeauftragten bestellt werden.[38]

---

33 Däubler in DKWW § 4f Rn. 31.

34 Simitis § 4f Rn. 103.

35 Taeger/Gabel Kommentar zum BDSG § 4f Rn 74; Bergmann/Möhrle/Herb § 4f Rn. 103.

36 Die BfDI, Info 4 „Die Datenschutzbeauftragten in Behörden und Betrieb“ S. 15.

37 Für den Leiter der EDV-Abteilung Simitis § 4f Rn. 100; Erfurter Komentar zum Arbeitsrecht BDSG §4f Rn. 5; Däubler DKWW § 4f Rn. 31; BfDI, Fn. 19, S. 14.

38 Statt vieler: Simitis § 4f Rn. 102 m.w.N; https://www.bfdi.bund.de/bfdi_wiki/index.php/Interessenkonflikte_nebenamtlicher_Datenschutzbeauftragter, zuletzt eingesehen am 10.04.2016.

8.5

Leiter der Revision können zu betrieblichen Datenschutzbeauftragten bestellt werden. Die gegenteilige Ansicht, die eine gleichzeitige Bestellung des Mitarbeiters der Revision als betrieblicher Datenschutzbeauftragter mit dem Argument ablehnt, der Revisor sei in erster Linie der Wirtschaftlichkeit verpflichtet[39], ist abzulehnen. Als Kontrolleure sind Mitarbeiter der Revision ihrem Revisionsauftrag verpflichtet, der sich keinesfalls ausschließlich in wirtschaftlichen Themenstellungen erschöpfen muss, sondern darüber hinaus auch die Prüfung betrieblicher und gesetzlicher Regelwerke umfassen kann.[40]

8.6.

Mitglieder der Mitarbeitervertretung können als betriebliche Datenschutzbeauftragte bestellt werden. Dies ergibt sich bereits aus den gleichgerichteten Interessen des Datenschutzbeauftragten und des MAV-Mitgliedes, die u. a. in der konsequenten Umsetzung des Datenschutzgesetzes bestehen.[41] Wollte man Mitarbeitervertreter generell als ungeeignet ansehen, würde dies auf eine Benachteiligung gegenüber anderen Arbeitnehmern hinauslaufen.[42] Seit einer Entscheidung des Bundesarbeitsgerichtes im Jahr 2011 ist diese Frage für Betriebsratsmitglieder entschieden.[43]

9. Bestellung einer Person für eine andere verantwortliche Stelle desselben Bistums

Wenn jede selbständige juristische Person einen betrieblichen Datenschutzbeauftragten zu benennen hat, soweit die weiteren Voraussetzungen gegeben sind (s.o. 5.), kann eine Person, die bei einer verantwortlichen Stelle beschäftigt ist, und dort wegen der von ihr wahrgenommenen Haupt-Tätigkeit für die Übertragung der Funktion des betrieblichen Datenschutzbeauftragten nicht geeignet ist dennoch betriebliche Datenschutzbeauftragte der anderen verantwortlichen Stelle sein. Z.B. kann der IT-Verantwortliche des Ordinariates zum betrieblichen Datenschutzbeauftragten des Caritasverbandes des Bistums bestellt werden. Ebenso könnte der Personalleiter des Caritasverbandes zum betrieblichen Datenschutzbeauftragten im Ordinariat bestellt werden. Der Interessenkonflikt, der diese Personen in der eigenen Stelle hindert die Funktion als betrieblicher Datenschutzbeauftragter zu übernehmen ist in der selbständigen Einrichtung, der er nicht angehört, nicht gegeben. Dies ergibt sich auch aus der Regelung des § 20 Abs. 3 a. E.

10. Bestellung

Die Bestellung hat gem. § 20 Abs. 1 schriftlich zu erfolgen. Dies gilt sowohl für eine Bestellung nach § 20 Abs. 1 als auch für eine solche nach § 20 Abs. 2, auch wenn dort das Schriftformerfordernis nicht ausdrücklich noch einmal wiederholt wird.

[39] Simitis § 4f Rn. 104.

[40] So im Ergebnis auch Däubler, DKWW § 4f, Rn. 31; Reinhard NZA 2013, 1049 ff.

[41] Für den Betriebsrat: Bommer ZD, 2015, 123; Däubler Gläserne Belegschaften? Rn. 596; eher ablehnend BfDI, Info 4 „Die Datenschutzbeauftragten in Behörden und Betrieb“ S. 16.

[42] Däubler DKWW § 4f Rn. 32; a. A. Bergmann/Möhrle/Herb § 4f Rn. 105.

[43] BAG v. 23.03.2011 – 10 AZR 562/09; NZA 2011,1036.

Die Schriftform ist konstitutiv. Ohne eine schriftliche Bestellung ist diese unwirksam. [44]
Eine Bestellung gegen den Willen des Arbeitnehmers ist nicht möglich, da sowohl die Bestellung als auch die Abberufung als betrieblicher Datenschutzbeauftragter eine Änderung des Arbeitsvertrages bedeuten, die vom Arbeitnehmer angenommen werden muss.[45] Aus diesem Grunde ist der h. M. zu folgen, nach der eine Bestellungsurkunde vom betrieblichen Datenschutzbeauftragten mit zu unterschreiben ist.[46]

11. Ende der Bestellung

Die Verweisung in § 20 Abs. 8 auf § 16 ist unglücklich. Einigkeit besteht wohl darüber, dass zur Berufung für den betrieblichen Datenschutzbeauftragten die Befähigung zum Richteramt nicht vorliegen muss.
Die in § 20 Abs. 8 angesprochenen „übrigen Voraussetzungen" betreffen dann die Befristung der Bestellung sowie den Widerruf der Bestellung.

11.1. Befristung

Die Bestellung des betrieblichen Datenschutzbeauftragten kann gem. § 16 Abs. 1 auf die § 20 Abs. 8 verweist nur befristet erfolgen. Dabei ist eine Befristung zwischen vier und acht Jahren möglich. Wenn in der Berufungsurkunde keine Frist festgeschrieben ist, ist im Sinne der Wahrung der Unabhängigkeit des Datenschutzbeauftragten von der längsten Frist auszugehen.

11.2. Abberufung

Eine Abberufung des betrieblichen Datenschutzbeauftragten ist gem. § 20 Abs. 8 nur in den Fällen des § 16 Abs. 3 möglich.

11.3. Amtsniederlegung

Darüber hinaus endet die Beauftragung, wenn der betriebliche Datenschutzbeauftragte sein Amt niederlegt. Dies ergibt sich aus der Verweisung von § 20 Abs. 8 auf § 16 Abs. 3 a. E. Statt des Bischofs hat die verantwortliche Stelle, die den betrieblichen Datenschutzbeauftragten bestellt hat die Bestellung zurück zu nehmen, wenn der betriebliche Datenschutzbeauftragte dies beantragt. Eine „Niederlegung" des Amtes ist als ein solcher Antrag zu verstehen.

---

[44] Simitis § 4f ,Rn. 59; Däubler § 4f Rn. 25.

[45] BAG vom 13.03.2007 -9 AZR 612/05, Der Betrieb 2007, 1198, 1200.

[46] Bergmann/Möhrle/Herb § 4f Rn. 55f.; Simitis § 4f Rn. 57; Däubler in DKWW § 4f Rn. 25; In der Info 4 der BfDI ist dies in dem Muster der Anlage 9 nicht berücksichtigt, jedoch auf der Internetseite der BfDI http://www.bfdi.bund.de/DE/Infothek/Gesetze_Rechtsprechung/RechtsprechungDS/BDSG_Allgemein/Artikel/130307_BAG_BestellungDatenschutzbeauftragter.html?__lang=en (zuletzt eingesehen 11.04.2016) ausdrücklich aufgeführt.

6.2 Veröffentlichung von Ehe- und Altersjubiläen in Presseerzeugnissen des Bistums oder der Pfarreien

[Beschluß der Konferenz der Diözesandatenschutzbeauftragten vom 19.-20. November 2016]

Die Konferenz der Diözesandatenschutzbeauftragten empfiehlt den (Erz-)Diözesen eine einheitliche, an den Regelungen des Bundesmeldegesetzes orientierte Jubiläumsordnung gemäß dem nachfolgenden Muster zu erlassen:

Jubiläumsordnung
Bei Alters- und Ehejubiläen, Geburten, Sterbefällen, Ordens- und Priesterjubiläen können Namen der Betroffenen und ggf. deren Wohnort (nicht die Straße) sowie der Tag und die Art des Ereignisses in den Publikationsorganen der Pfarreien (Pfarrnachrichten) sowie in den kircheneigenen Printmedien veröffentlicht werden, wenn die Betroffenen der Veröffentlichung nicht schriftlich oder in sonstiger geeigneter Form bei der zuständigen Pfarrei widersprochen haben.
Auf das Widerspruchsrecht ist mindestens einmal jährlich in den Publikationsorganen der Pfarreien bzw. in den kircheneigenen Printmedien hinzuweisen. Der Hinweis ist im äußeren Erscheinungsbild von dem Rest des Textes der Veröffentlichung hervorzuheben. Ein bei der Pfarrei eingereichter Widerspruch ist unverzüglich der Meldestelle des Bistums mitzuteilen.

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

Soll eine weitere über die genannten Medien hinausgehende Veröffentlichung, insbesondere eine solche im Internet erfolgen, ist die vorherige Zustimmung der Betroffenen einzuholen.

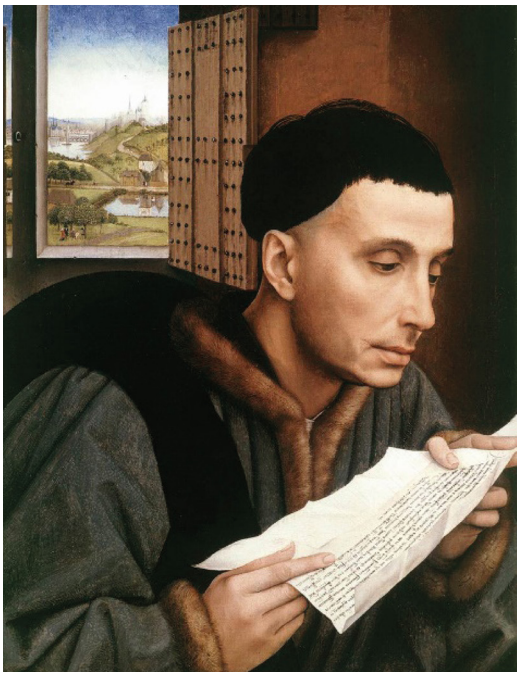
Die Meldestelle des Bistums ist berechtigt, auf Anfrage einer der genannten Stellen die entsprechenden Daten zu übermitteln. Die Pfarreien sind berechtigt, die entsprechenden Daten an ein kircheneigenes Printmedium zu übermitteln.

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

Aus Sicherheitsgründen ist auf die Veröffentlichung der Straßenanschrift zu verzichten. Ein „kircheneigenes Printmedium“ ist derzeit die Kirchenzeitung.

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
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
VDD	Verband der Diözesen Deutschlands
VwVfG	Verwaltungsverfahrensgesetz



Hl. Ivo

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

Quelle Foto: Joachim Schäfer – www.heiligenlexikon.de

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

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