Kirchliches Datenschutzrecht

(Jupp Joachimski)

Bearbeitungsstand 01.04.2020

Vorbemerkung:

Diese Einführung in das Datenschutzrecht soll es kirchlichen Mitarbeitern, Ordensangehörigen und Ehrenamtlichen erleichtern, sich in das Datenschutzrecht einzuarbeiten. Sie gilt im Prinzip durchaus bundesweit; die Leser mögen es mir jedoch nachsehen, wenn ich für Beispiele des Landesrechts jeweils die bayerischen heranziehe. Die Einführung sollte zweckmäßigerweise am Computer gelesen werden, damit die Links jederzeit aufgerufen werden können. Neu bestellte betriebliche Datenschutzbeauftragte sollten dieses Skriptum vor der „Einführungshilfe für den betrieblichen Datenschutzbeauftragten[1]“ lesen.

Prinzipien des Datenschutzrechts

Was unterfällt dem Datenschutzrecht?

Grundsätzlich sind nur personenbezogene Daten Gegenstand des Datenschutzrechts. Eine Legaldefinition dafür gibt es in § 4 Nr. 1 Kirchliches Datenschutzgesetz:

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen.

Das bedeutet: Alle Informationen, die sich einer bestimmten Person zuordnen lassen, also Familienname, Vorname, Geburtsdatum, Telefonnummer, Anschrift, aber auch Angaben, die weiter entfernt liegen, zum Beispiel Jahr der Schulentlassung, Autokennzeichen, Verwandtschaftsverhältnis einer bestimmten Person usw.

Identifizierte Personen sind solche, die aufgrund der bezeichneten Angaben klar definiert sind. **Identifizierbare** Personen sind solche, bei denen zwischen der Nennung der Angaben und der Erkenntnis, welche Person gemeint ist, noch ein Ermittlungsvorgang liegt, so zum Beispiel die Zuordnung eines bestimmten Autokennzeichens zu einem Halter; sie verlangt eine Auskunft aus dem Halterverzeichnis.

Natürliche Person ist im Gegensatz zur juristischen Person zu verstehen: Unter das Datenschutzrecht fallen also nicht die juristischen Personen des bürgerlichen Rechts (Vereine), des Handelsrechts (Aktiengesellschaften und Gesellschaften mit beschränkter Haftung) und des öffentlichen Rechts (Gemeinden, Landkreise, Bundesländer und Behörden). Zu der Eigenschaft „natürliche Person“ gehört es, dass die natürliche Person lebt. Tote genießen keinen Datenschutz!
Merksatz: *Der Datenschutz endet am Friedhofstor*.

Die Form der Daten

ist für den Datenschutz prinzipiell gleichgültig. Die Datenschutzregeln sind gleichermaßen anwendbar auf die Speicherung in Papierform oder in EDV-Form, § 4 Nr. 3 KDG. Es gibt lediglich dort Sonderregelungen, wo es um die Überwachung einer automatisierten Verarbeitung geht.

Was ist mit Bildern oder Filmen?

[1] Zu finden auf der geschützten Downloadseite des Erzbischöflichen Ordinariats München. Zugangsberechtigungen erhalten Sie auf Anfrage von mir: jjoachimski@eomuc.de

Abbildungen von Personen fallen dann unter das Datenschutzrecht, wenn sie eine Identifizierung der jeweiligen Person ermöglichen. Deswegen war es notwendig, das Recht einer Person an ihrer Abbildung gesondert zu regeln. Dies geschah im Kunsturhebergesetz, §§ 22 ff. Auch im kirchlichen Bereich ist diese Vorschrift anzuwenden, weil es keine Sonderregelung dafür gibt. Wegen der Sachnähe werden die Rechte an Bildern oder Filmen auch von den Datenschützern behandelt; hier wird die Materie auf den Seiten 14f. besprochen.

Die Videoüberwachung (§ 52 KDG) ist des Zusammenhangs wegen auch in der kirchlichen Datenschutzordnung (bzw. dem BDSG) geregelt, obwohl bei der Videoüberwachung nur mittelbar personenbezogene Daten betroffen sind.

Woher stammt der Datenschutz?

Die Diskussion um das Recht des Staates, im Rahmen der Erhebungen zur Volkszählung 1982 die Daten der Bürger zu erheben, mündete in entsprechenden gesetzlichen Regelungen auf allen Ebenen. Es war wohl das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983, welches ein neues – bisher nicht im Grundgesetz stehendes – Grundrecht der Bürger schuf, das **Recht auf informationelle Selbstbestimmung.**

„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Die Katholische Kirche hatte sogar schon im Vorfeld am 25.1.1983 mit can. 220 CIC ein Fundamentalrecht auf Datenschutz geschaffen:

"Niemandem ist es erlaubt, den guten Ruf, den jemand hat, rechtswidrig zu schädigen und das Recht irgendeiner Person auf Schutz der eigenen Intimsphäre zu verletzen."

Welche Grundprinzipien hat der Datenschutz?

Unabhängig von der anzuwendenden Rechtsordnung hat der Datenschutz **drei Grundprinzipien**:

- **Datensicherheit**
- **Schutz gegen unbefugte Kenntnisnahme**
- **Auskunftspflicht**

Diese Grundprinzipien sind in allen Datenschutznormen geregelt. Sie stellen sozusagen das „Skelett" des Datenschutzes dar. Es gibt Bestrebungen, diese Grundprinzipien auszuweiten, zum Beispiel in der Erklärung von Montreux vom 16. September 2005:

- Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten
- Richtigkeit
- Zweckgebundenheit
- Verhältnismäßigkeit
- Transparenz
- individuelle Mitsprache, namentlich Garantie des Zugriffsrechts für die betroffenen Personen
- Nicht-Diskriminierung
- Sicherheit
- Haftung
- unabhängige Überwachung und gesetzliche Sanktionen
- angemessenes Schutzniveau bei grenzüberschreitendem Datenverkehr

Welche rechtlichen Vorschriften sind anzuwenden?

Das Datenschutzrecht ist deswegen besonders kompliziert, weil es in verschiedenen rechtlichen Ebenen Regelungen dazu gab, die sich jüngst erst stark durch eine Verordnung der Europäischen Union (EU-Datenschutz-Grundverordnung – EU-DS-GVO) veränderten:

Die **Bundesrepublik Deutschland** hatte erstmals 1983 eine Datenschutzregelung erlassen, das Bundesdatenschutzgesetz[2]. Im kirchlichen Bereich ist es nicht anzuwenden, weil die Sonderregelung des kirchlichen Datenschutzgesetzes vorgeht. Das Bundesdatenschutzgesetz hat durch die EU-DS-GVO weitgehend seine Bedeutung verloren. Es enthält nun im Wesentlichen Ausnahmen und Ergänzungen zur EU-DS-GVO.

Neben dem Bundesdatenschutzgesetz hat der Bund in anderen Gesetzen Datenschutzregelungen geschaffen. Die wichtigsten sind die über das Sozialgeheimnis in § 35 Abs. 1 SGB I sowie die beruflichen Geheimhaltungspflichten nach § 203 StGB.

Die **Bundesländer** hatten parallel zum BDSG jeweils eigene Datenschutzvorschriften erlassen. Diese Landesdatenschutzgesetze galten ausschließlich für die jeweiligen Landesbehörden, haben inzwischen aber auch viel an Bedeutung verloren, weil die EU-DS-GVO dort direkt eingreift. Neben diesen Datenschutzgesetzen gibt es noch besondere Regelungen in den einzelnen Bundesländern für bestimmte Fachgebiete; sie bleiben erhalten. Am wichtigsten sind die Regelungen für das Schulwesen (Beispiel: Art. 85 des bayerischen Gesetzes über Erziehung und Unterricht) und die Krankenhäuser (Beispiel: Art. 27 des bayerischen Gesetzes über das Krankenhauswesen).

Die **Europäische Union** hatte 1995 eine Richtlinie zum Datenschutzrecht erlassen, welche nicht unmittelbares Recht wurde, sondern lediglich die Mitgliedstaaten band. Sie waren verpflichtet, ein nationales Datenschutzrecht zu erlassen, das die Mindeststandards der europäischen Richtlinie einhielt, was aber nicht überall geschah. Es gab Staaten, die sich einen wirtschaftlichen Vorteil durch Nichtumsetzung der Richtlinie verschafften.

Dem begegnete die Europäische Union mit der **Datenschutz-Grundverordnung**, welche im Gegensatz zur Richtlinie unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union ist. Sie tritt am 25.5.2018 in Kraft. Den Text dieser Grundverordnung[3] kann man herunterladen. Von Bedeutung ist für uns insbesondere Art. 91, der die Garantie der Weimarer Reichsverfassung und des Grundgesetzes für den EU-Bereich fortschreibt:

Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.

In Art. 137ff. der Weimarer Reichsverfassung war den „Religionsgesellschaften“ das Recht der Selbstverwaltung vorbehalten. Dieses Recht hatte schon das Grundgesetz in Art. 140 für die Bundesrepublik Deutschland fortgeschrieben. Soweit die Selbstverwaltungshoheit des Grundgesetzes reichte, dürfen insbesondere die Kirchen, also die evangelische und katholische Kirche, ihre inneren Angelegenheiten selbst verwalten. Zu diesen zählte nach ganz allgemeiner Meinung auch das Datenschutzrecht.

In Ausübung dieses Selbstverwaltungsrechts hatten die beiden großen christlichen Kirchen entsprechende Normen zum Datenschutz erlassen. Sie waren auch deswegen notwendig, weil nach § 15 Abs. 4 BDSG eine Übermittlung von Daten durch staatliche Behörden an öffentlich-rechtliche Religionsgesellschaften nur dann zulässig ist, wenn bei ihnen ausreichende Vorkehrungen für den Datenschutz getroffen sind. Das bedeutet: Der Bundesgesetzgeber ging davon aus, dass auch die Kirchen kein rechtsfreier Raum sind, was den Datenschutz betrifft. Sie müssen sich bemühen, ein dem staatlichen Datenschutzrecht gleichwertiges Recht für ihren Bereich zu schaffen. Nur dann bleibt Ihre Selbstverwaltungshoheit in dieser Hinsicht erhalten.

[2] Der hier vorhandene Link verweist auf eine Textdarstellung, welche die EU-DS-GVO und das neue BDSG anzeigen kann.
[3] Der hier vorhandene Link verweist wieder auf die Textdarstellung, welche die EU-DS-GVO und das neue BDSG anzeigen kann.

Übersicht: Datenschutzrecht der Kirchen in Deutschland

- In der **katholischen Kirche**: KDG = Gesetz über den kirchlichen Datenschutz, mit KDG-DVO anwendbar auf alle kirchlichen Rechtsträger, unabhängig von ihrer Organisationsform, also Bistümer, Gemeinden, Caritas, Anstalten, Orden etc., weitgehend dem BDSG nachgebildet, große Teile wörtlich, wortgleich in jedem Bistum in Kraft gesetzt. *Quelle: Webseite des jeweiligen Bistums oder www.erzbistum-muenchen.de/datenschutz*

  Durchführungsverordnung: https://www.erzbistum-muenchen.de/cms-media/media-45173820.pdf

  In den Ordensgemeinschaften päpstlichen Rechts gilt statt des KDG die Kirchliche Datenschutzreglung für Ordensgemeinschaften. Sie ist bis auf wenige Regelungen für den Ordensdatenschutzbeauftragten wortgleich mit dem KDG; Fundstelle: https://www.orden.de/fileadmin/user_upload/KDR-OG_Beschluss_30_01_18.pdf
- **Evangelische Kirche**: Datenschutzgesetz der EKD vom 12. November 1993 (ABl.EKD S. 505), geändert durch Kirchengesetz vom 1.1.2013, ABl. EKD 2013 S. 2.
  Quelle: https://datenschutz.ekd.de/datenschutzrecht/ekd/
- Nach Art. 91 des Entwurfes der neuen EU-Datenschutzverordnung bleiben diese Regelungen auch nach Inkrafttreten der Verordnung gültig, wenn sie „im Einklang" mit der Verordnung stehen. Darunter wird ein Zustand der Gleichwertigkeit verstanden.

Alle Regelungen des kirchlichen Datenschutzes sind an die EU-DS-GVO angelehnt, können jedoch nicht diese in vollem Umfang abbilden. Das Datenschutzrecht der katholischen Kirche hat im Gegensatz zu demjenigen der evangelischen Kirche auch noch die Besonderheit, dass es keine parlamentarische Kontrolle (in der evangelischen Kirche durch die Synode) gibt. Diese Besonderheiten der Regelungen in der katholischen Kirche ändern jedoch nichts daran, dass das Datenschutzrecht der katholischen Kirche dem staatlichen zwar nicht gleichartig, aber doch gleichwertig ist. Es wird nämlich an verschiedenen Stellen die Datenschutzregelung der EU-DS-GVO übertroffen.

Die wichtigsten Regelungen des Kirchlichen Datenschutzgesetzes

Wo gilt das KDG?

Die Frage ist in § 3 geregelt:

§ 3 Organisatorischer Anwendungsbereich

(1) *Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch folgende kirchliche Stellen:*

a) die Diözese, die Kirchengemeinden, die Kirchenstiftungen und die Kirchengemeindeverbände,

b) den Deutschen Caritasverband, die Diözesan-Caritasverbände, ihre Untergliederungen und ihre Fachverbände ohne Rücksicht auf ihre Rechtsform,

c) die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform.

Zu § 3 Abs. 1:

In dieser Vorschrift wird der sachliche Geltungsbereich festgelegt. Der örtliche Geltungsbereich ergibt sich automatisch aus der Struktur der kirchlichen Gesetzgebung: Eine kirchliche Anordnung des Diözesanbischofs gilt automatisch nur innerhalb des Bistums und umfasst die im Bistum ansässigen Ordensgemeinschaft bischöflichen Rechts. Für Ordensgemeinschaften päpstlichen Rechts gilt eine Anordnung des Ordensoberen innerhalb des Ordens bundesweit und zwar auch dann, wenn der Orden im Ausland Niederlassungen hat. Ob eine Ordensgemeinschaft bischöflichem oder päpstlichem Recht unterfällt, lässt sich auf der Webseite der Deutschen Ordensobernkonferenz klären.

Für kirchliche Dienststellen ist Abs. 1 eindeutig; sie unterfallen immer dem KDG. Kritisch wird es jedoch nach § 1 Abs. 1c, soweit sich die Kirche privatrechtlicher Organisationsformen bedient. Zu diesen zählen diejenigen des bürgerlichen Rechts (Verein) oder des Handelsrechts (Aktiengesellschaft, Gesellschaft mit beschränkter Haftung, Genossenschaft u. ä.). Das KDG gilt für derartige Organisationsformen jedoch nur dann, wenn die so genannte „Kirchlichkeitsprüfung“ erfüllt wird. Eine derartige Organisation ist nur dann eine kirchliche Dienststelle im Sinne des KDG, wenn sie nach kirchlichem Selbstverständnis ihrem Zweck oder ihrer Aufgabe entsprechend zur Mitwirkung an der Erfüllung des kirchlichen Auftrags berufen ist.

Beispiele: Eine Schule, ein Kindergarten oder ein Krankenhaus zählen durchaus zur Erfüllung des kirchlichen Auftrags. Dagegen ist eine Mineralwasser- Vertriebs-Gesellschaft nicht ohne weiteres eine kirchliche Dienststelle, auch wenn sie von der Kirche oder einer Ordensgemeinschaft betrieben wird. Ein besonderer Streitfall ist häufig die Kirchenzeitung. Bei ihr wird zu prüfen sein, ob die Gewinnerzielung im Vordergrund steht oder die Kommunikation mit den Mitgliedern der Kirche, ersteres wohl der Regelfall.

Geltung anderer Rechtsnormen

Nach ihrem eigenen Verständnis ist das kirchliche Datenschutzgesetz gegenüber spezielleren Vorschriften subsidiär, d.h. nicht das KDG, sondern diese Vorschriften sind anzuwenden (§2 Abs.2 KDG). Das gilt insbesondere im Verhältnis zu

- den Vorschriften der kirchlichen Archivordnung
- landesgesetzlichen Vorschriften über den Datenschutz in Krankenhäusern und Schulen

Die Rechtmäßigkeit des Umgangs mit den Daten

Ausgangspunkt dafür ist

§ 6 Rechtmäßigkeit der Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Dieses Gesetz oder eine andere kirchliche oder eine staatliche Rechtsvorschrift erlaubt sie oder ordnet sie an;

b) die betroffene Person hat in die Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt;

c) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

d) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

e) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

f) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im kirchlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

g) *die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um einen Minderjährigen handelt. Lit. g) gilt nicht für die von öffentlich-rechtlich organisierten kirchlichen Stellen in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.*

Diese Vorschrift ist die zentrale Handlungsanweisung des KDG. Sie unterscheidet sich ganz elementar von der sonstigen deutschen Rechtsordnung. Diese sieht nämlich in zahlreichen Gebieten des Verwaltungs- oder Nebenstrafrechts vor, dass eine Handlung grundsätzlich legal ist, wenn eine entsprechende Erlaubnis vorliegt. Im Datenschutzrecht ist es genau anders herum: Der Umgang mit Daten ist grundsätzlich illegal, es sei denn … Das mag haarspalterisch klingen, ist (es) aber durchaus von Bedeutung: Bleibt unklar, ob eine Aufgabe vorliegt, ist im Zweifel anzunehmen, dass sie fehlt.

Die Befugnis zum Umgang mit Daten folgt also unmittelbar aus einer entsprechenden Aufgabe. Es muss daher immer zuerst geprüft werden, ob die kirchliche Dienststelle eine entsprechende Aufgabe zum Umgang mit diesen speziellen Daten hat. Das hat nichts mit dem eher als verwerflich anzusehenden Grundsatz „Der Zweck heiligt die Mittel“ zu tun, weil für das KDG (und das BDSG) entscheidend ist, ob der Umgang mit diesen Daten objektiv, also aus der Sicht eines unbeteiligten Dritten, erforderlich zur Erfüllung der Aufgaben ist.

Die **allgemeine Prüfungsreihenfolge für den Umgang einer Dienststelle mit Daten** ist daher:

1. Liegt eine entsprechende Aufgabe (objektiv) vor?
2. Besteht sonst ein Rechtfertigungsgrund nach § 6 Abs. 1 KDG für Verarbeitung von Daten, insbesondere: Hat der Betroffene eingewilligt?

Diese allgemeine Prüfungsreihenfolge gilt für jede Art von Umgang mit Daten. Hierbei ist zu beachten, dass nicht nur die Weitergabe der Daten, sondern schon deren Aufnahme (Speicherung), interne Auswertung und Veränderung unter das Verbot mit Ausnahmen fällt.

Die Schutzbereiche des kirchlichen Datenschutzes

Hierbei ist zu beachten, dass jede datenrelevante Handlung einer kirchlichen Dienststelle zwei Richtungen haben kann: Richtet sich die Handlung nach außen, betrifft sie also die „Klienten“ der Kirche, gelten die allgemeinen Regeln. Besondere Regeln gelten dann, wenn die Handlungen der Kirche ihre eigenen **Mitarbeiter** betreffen. In diesem Fall gibt es eine weitere Einschränkung jeder Art des Umgangs mit Daten nach § 53 KDG, vgl. dazu die Ausführungen unten.

Die Begriffsbestimmungen

In § 4 KDG entsprechen die Definitionen überwiegend der Regelung in der EU-DS-GVO. Die Vorschrift sollte immer beachtet werden, wenn die Bedeutung eines Begriffes unklar ist. Aus den zahlreichen Begriffsbestimmungen sollen zwei herausgehoben werden:

- Die besonderen Kategorien der personenbezogenen Daten (§ 4 Nr.2 KDG) kennzeichnen, welche Daten besonders empfindlich sind. Sie bedürfen sowohl bei der Speicherung wie auch bei der Übermittlung besonderen Schutzes. Derartige Daten dürfen keinesfalls per E-Mail übermittelt werden; werden sie in Papierform vorgehalten, so müssen die entsprechenden Unterlagen immer in verschließbaren Behältnissen aufbewahrt werden.
- Der Begriff der Beschäftigten in § 4 Nr. 24 trägt den Besonderheiten der katholischen Kirche Rechnung. Es ist zu beachten, dass unter dem Begriff der Beschäftigten auch Kleriker fallen. Das bedeutet im Ergebnis, dass auch sie auf das Datengeheimnis nach §5 Satz 2 KDG verpflichtet werden müssen.

Datenverarbeitung

Sprach das Bundesdatenschutzgesetz in seiner bis 24. Mai 2018 gültigen Fassung noch von verschiedenen Formen des Umgangs mit Daten, so ist mit Inkrafttreten des KDG eine ganz erhebliche Änderung eingetreten: Unter Verarbeitung versteht man nach § 4 Nr. 3 KDG jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Ab-

gleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Im Ergebnis ist also jeder Umgang mit Daten eine Verarbeitung, insbesondere auch die Erhebung.

Diese Begriffsbestimmung sagt noch nichts darüber aus, von wem die Daten über den Betroffenen letztendlich stammen. Sie können von ihm selbst oder auch von Dritten kommen. Lediglich bei Arbeitnehmern gibt es den Grundsatz, dass die Daten des Arbeitnehmers durch den Dienstgeber prinzipiell bei ihm selbst zu erheben sind.

Hierzu kommt der allgemeine Grundsatz des Datenschutzrechts, dass **Daten nur für den Zweck verwendet werden dürfen, für den sie erhoben sind**.

Beispiel: *Nach § 42 BMeldeG darf die Kirche auf die staatlichen Meldedaten zugreifen. Dieses Recht ist ihr eingeräumt, um die Kirchensteuerpflicht durchzusetzen. Für arbeitsrechtliche Zwecke darf die Kirche diese Daten jedoch nicht verwenden, z.B., um festzustellen, ob ein Arbeitnehmer geschieden ist.*

Datensicherheit

Die erhobenen Daten muss die Dienststelle nach § 7 Abs. 1f KDG so sichern, dass

- sie bei Bedarf zur Verfügung stehen und
- ein Zugriff unbefugter Dritter mit der notwendigen Sicherheit ausgeschlossen werden kann.

§ 7 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Was bedeutet diese Vorschrift?

Eigentlich müsste das KDG Tausende oder gar Millionen von Situationen schildern und jeweils darlegen, welche Sicherheitsmaßnahmen für die Daten erforderlich sind. Das tut sie nicht. Sie begnügt sich vielmehr damit, die Abwägung darzustellen, vor der die kirchliche Dienststelle steht. Es bleibt also der Würdigung im Einzelfall überlassen, was an Sicherheitsmaßnahmen für die Daten erforderlich ist. Ich habe im Laufe meiner Praxis viele Situationen kennengelernt, von denen ich einige hier beschreiben will, um zu zeigen, was bei einer Abwägung zu berücksichtigen ist:

- **Personalakten**: Sie sind immer sicherheitsempfindlich und müssen deswegen zumindest in verschlossenen Aktenschränken aufbewahrt werden.
- **E-Mail:** Einerseits ist der E-Mail-Verkehr tatsächlich höchst unsicher, weil ohne großen Aufwand E-Mails abgefangen werden können, andererseits ist er furchtbar praktisch. Bei der Abwägung wird aber sicher zu berücksichtigen sein, dass das größte Risiko für den Datenschutz dann besteht, wenn die Daten beim Provider durchlaufen. Dort kann sie jeder Mitarbeiter lesen. Deswegen ist der dienstliche E-Mail-Verkehr mit Dritten dann zu unterlassen, wenn kein entsprechendes Einverständnis des Dritten vorliegt und die Daten über einen nicht kirchlichen oder nicht staatlichen Server laufen.
- **Voice Over IP:** Der Grund dafür, dass bei Internetprovidern Telefonanschlüsse so günstig sind, liegt in der Übertragungsart. Wird nämlich ein Telefongespräch über das Internet abgewickelt, so verursacht es so gut wie keine Leitungskosten. Natürlich hat das seinen Nachteil, weil auf diese Weise die Abhörsicherheit sehr gering ist. Auch in diesem Fall wird eine Abwägung zu treffen sein und es muss sicher z.B. auch berücksichtigt werden, dass das Interesse von Kriminellen am Telefonverkehr des Pfarrbüros eher gering ist. Deswegen ist prinzipiell nichts dagegen einzuwenden, dass auch das Pfarrbüro die kostengünstige Variante von VoIP wählt. Bei einer Telefonseelsorge wird man mit dieser Argumentation nicht weit kommen.

- **Dienstliche Daten auf dem Privat-PC:** Das ist sicher sehr kritisch zu sehen. Andererseits ist bei bestimmten Berufsgruppen wie zum Beispiel Lehrern an kirchlichen Schulen oder teilzeitbeschäftigten Pfarrsekretärinnen ein gänzliches Verbot häufig nicht durchzusetzen. Um die Sicherheit zu erhöhen, kann man zu Hilfsmitteln greifen und zum Beispiel eine Bildschirmsperre nach 10 Minuten eingreifen lassen. Bei Laptops verhindert zum Beispiel ein Fingerabdrucksensor, dass Unbefugte sofort auf die Daten zugreifen können.
- **Daten in der Cloud**: Unter dem Begriff „Cloud" versteht man die Datenspeicherung auf einem fernen Datenspeicher wie zum Beispiel Dropbox, Microsoft One Drive o.ä. Diese Art von Datenspeicherung ist nicht grundsätzlich unsicher; maßgeblich ist jedoch, wo sich der physikalische Datenspeicher befindet. Ist dieser im EU – Ausland, dürfen kirchliche Dienststellen derartige Datenspeicher nicht verwenden. Dropbox und Microsoft One Drive scheiden daher aus. Aus dem gleichen Grund ist die Verwendung von Microsoft Office 365 unzulässig, weil die Standarddatenspeicherung bei diesem Programm ebenfalls im Ausland stattfindet. Alternativen sind T-Online Mediencenter (25 GB gratis) oder 1&1. Für größere Dienststellen ist es noch besser, eine vorhandene gemeinsam genutzte Festplatte mit dem Programm „Own Cloud" zum fernen Datenspeicher auszubauen. Näheres dazu steht in den Hinweisen der Downloadseite.
- **Kommunikation über What's App oder Facebook**: Die sozialen Netzwerke leben davon, dass sie die Kontakte der Nutzer zu Werbezwecken ausschlachten. Die Kommunikation über derartige soziale Netzwerke ist daher in hohem Maße unsicher und auch deswegen nicht für dienstliche Zwecke brauchbar, weil die Datenzwischenspeicherung im EU-Ausland stattfindet. Gerade bei den Messengern gibt es aber preisgünstige oder gar kostenfreie Alternativen wie zum Beispiel Threema oder Free Message. Man muss auch immer bedenken, dass es in Deutschland schon Gerichtsurteile gegeben hat, in denen Nutzer von What's App deswegen zu Schadensersatzzahlungen verurteilt wurden, weil die bei ihnen gespeicherten Kontakte an Facebook weitergeleitet wurden. Das kann vernünftigerweise ein Arbeitgeber nicht hinnehmen.

Es verlangt von Ihnen jedoch niemand, dass Sie über all das auswendig Bescheid wissen. Gerade zu dem Thema „elektronische Kommunikation" gibt es ein Merkblatt in der Downloadseite, in welchem all das erklärt wird.

Beim Lesen ist vielleicht auch zu erkennen, dass jeder datenschutzrechtliche Eingriff eine Menge an Überlegungen verlangt. Es gibt in diesem Bereich keine schwarz-weißen Entscheidungen, sondern nur die Ergebnisse einer sorgfältigen Abwägung. Sinnvoll ist es natürlich, diese Abwägung zu einem Zeitpunkt zu betreiben, zu dem man auch die notwendige Zeit hat. Deswegen sieht die Ausführungsverordnung zur KDG vor, dass alle Leiter kirchlicher Dienststellen möglichst einmal im Jahr sich Gedanken zum Thema Datenschutz machen sollen. Das Ergebnis dieser Gedanken nennt man das

Datenschutzkonzept

In ihm wird festgestellt, mit welchen Daten die Dienststelle umgeht und welchen Risiken diese Daten ausgesetzt sind. Nahezu automatisch ergibt sich dann, welche Abwehrmaßnahmen die Dienststelle gegen den Verlust von Daten oder ihre Unsicherheit treffen muss. Ein Muster für ein Datenschutzkonzept der Kirchenstiftungen finden Sie in der Downloadseite des erzbischöflichen Ordinariats München im Ordner „Kirchenstiftungen". Man sollte dieses Muster aber nicht nur abschreiben, sondern die Gelegenheit nutzen, eine Bestandsaufnahme zu fertigen.

Verpflichtungserklärung

Zu den organisatorischen Maßnahmen im Sinne des § 7 KDG gehört es auch, dass die mit den Daten befassten Personen sich zum Schutz des Datengeheimnisses verpflichtet haben. Diese Verpflichtung ist in § 5 Satz 2 KDG vorgeschrieben und erstreckt sich auf alle Personen, die mit Daten zu tun haben. Hierzu zählen auch Kleriker bzw. Ordensangehörige ebenso wie Ehrenamtliche. Gerade bei letzteren ist nicht zu verkennen, dass sie vielfach die Unterzeichnung einer Verpflichtungserklärung als Zumutung empfinden. Es bedarf häufig der näheren Erläuterung, warum auch sie diese Verpflichtungserklärung abgeben müssen. Meist hilft der Hinweis darauf, dass die staatlichen Anforderungen eine Vorgabe auch für die Kirche bilden. Ausfüllbare Muster für Verpflichtungserklärungen finden sich auf der erwähnten Downloadseite.

Die Rechtfertigung des Umgangs mit Daten

Der Umgang mit Daten ist gemäß § 5 KDG nur dann zulässig, wenn eine Rechtfertigung gemäß § 10 KDG vorliegt. In dieser Vorschrift bildet wiederum Abs. 1 Satz 1 die zentrale Norm. Es ist also in jedem Fall zu prüfen, ob die beabsichtigte Verarbeitung der Daten – Erheben, Speichern, Verändern oder Offenlegen – notwendig ist, um Aufgaben der Dienststelle zu erfüllen. Auch dafür gibt es keine generelle Überlegung; vielmehr muss am Einzelfall abgeleitet werden, warum das so ist.

Beispiele:

1. *In die Ministrantenliste eines Pfarrbüros soll der Familienstand der Eltern der jeweiligen Ministranten aufgenommen werden.*
   Hierfür gibt es keine Aufgabe, weil es für die Tätigkeit der Ministranten keine Rolle spielen kann, ob deren Eltern verheiratet, ledig oder geschieden sind. Die Auswirkung dieser Umstände ist derart mittelbar, dass ihre Kenntnis für die Auswahl und Beaufsichtigung der Tätigkeit der Ministranten unerheblich ist.
2. *Eine Kirchenstiftung will die Namen ihrer Ministranten zusammen mit deren Anschriften auf ihrer Webseite nennen.*
   Hier könnte von einer Aufgabe der Kirchenstiftung gesprochen werden, wenn es um die bloßen Namen der Ministranten im Hinblick auf ihre Einteilung zu den verschiedenen Messen ging. Ganz eindeutig wird die Befugnis jedoch nicht, weil die Ministranten auch einzeln benachrichtigt werden können. Ganz sicher nicht zulässig (ohne die Einwilligung der jeweiligen Sorgeberechtigten) ist die öffentliche Nennung der Anschriften. Jede Veröffentlichung ist eine Mitteilung an Dritte im Sinne des § 12 KDG. Dafür gibt es keine entsprechende Aufgabe der Kirchenstiftung.
3. *Die Caritas will die Kirchenmitglieder im Bereich einer Kirchenstiftung mit der Bitte um Spenden anschreiben und fragt die Kirchenstiftungen nach deren Anschriften.*
   Die Caritas ist eine Organisation der Kirche im Sinne des § 3 Abs.1c KDG. Eine Offenlegung der Daten an sie richtet sich daher nach § 9 KDG. Gemäß § 9 Abs. 3 Satz 2 KDG muss die Kirchenstiftung nicht selbst prüfen, ob bei der Caritas eine entsprechende Aufgabe vorliegt. Abgesehen davon wäre diese Voraussetzung gegeben, weil es die Aufgabe der Caritas ist, zu helfen und natürlich die dafür erforderlichen Mittel aufzubringen.

Die Frage, ob in einer bestimmten Situation eine Aufgabe der kirchlichen Dienststelle vorliegt, kann schwierig sein. Gerade in solchen Zweifelsfällen bietet es sich an, die Auskunft des Diözesandatenschutzbeauftragten zu erholen.

In den oben bezeichneten Beispielen ging es schon teilweise um die

Offenlegung von Daten

Werden die Daten von der Dienststelle weitergegeben, so müssen zusätzlich zur Prüfung der Aufgabe im Sinne des § 6 KDG die §§ 9 und 10 KDG bemüht werden.

Zu prüfen ist also: Gehen die Daten an eine

Kirchliche oder staatliche Stelle (§ 9 KDG) oder	**einen Dritten bzw. an die ganze Welt (Fall der Veröffentlichung) § 10**
§ 9 Abs. 1: Wiederum ist die Aufgabe der Ausgangs- oder Empfangsstelle entscheidend.	Entscheidend ist die Aufgabe der Ausgangsstelle oder das berechtigte Interesse des Dritten.

Besonders zu beachten ist im Falle des § 9 dessen Abs.2 S.2-4:

Erfolgt die Offenlegung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung. In diesem Falle prüft die offenlegende Stelle nur, ob das Ersuchen im Rahmen der Aufgaben der empfangenden kirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

Das heißt im Klartext: Fordert eine andere kirchliche Stelle oder eine öffentliche (Gemeinde, Landratsamt) von der kirchlichen Stelle Daten an, so muss diese nicht prüfen, ob die Anforderung gerechtfertigt ist.

Beispiel: *Die staatliche Schule bittet den kirchlichen Kindergarten um Überlassung der Akten eines Kindes, das jetzt in die Schule kommt. Die Schule ist eine öffentliche Dienststelle und steht nach § 9 Abs.5 KDG einer kirchlichen Dienststelle gleich. Der Kindergarten kann ihr ohne weitere Bedarfsprüfung die Akten zugänglich machen.*

In einigen Fällen verdichtet sich die bloße Möglichkeit der Weitergabe von Daten an staatliche Stellen fast zu einer Verpflichtung, nämlich dann, wenn es um die Auskunft im **Ermittlungs- und Strafverfahren** geht. Eine kirchliche Dienststelle muss auch im Ermittlungs- und Strafverfahren nicht prüfen, ob die Auskünfte, die die Polizei oder die Staatsanwaltschaft von ihr verlangen, zu geben sind. Allerdings hat sie diese Prüfungsbefugnis immer, wird von ihr jedoch nur unter den Umständen Gebrauch machen, unter denen auch eine öffentliche Behörde entsprechend § 96 S. 1 StPO die Herausgabe von Unterlagen verweigern würde. Dies wäre nur dann der Fall, wenn die Herausgabe oder Auskunftserteilung dem Wohl der Kirche nachhaltigen Schaden zufügen würde.

Datenverkehr mit dem Ausland

Erstmals regelt das KDG auch den Datentransfer in das Ausland. Der Auslandsbezug zwingt deswegen, weil der Datenschutz nicht überall auf der Welt gleich ausgestaltet ist, die übermittelnde kirchliche Dienststelle zu einer sorgfältigen Zulässigkeitsprüfung. Dabei muss klargestellt werden, dass es sich um eine zusätzliche Prüfung der Zulässigkeit handelt, die allgemeinen Übermittlungsvoraussetzungen also bereits gegeben sein müssen, bevor überhaupt in diese Prüfung eingetreten wird.

Die Prüfung der Zulässigkeit von Datenübermittlungen in das Ausland geht in drei Schritten vor sich:

- Liegt ein Angemessenheitsbeschluss nach § 40 Abs. 1 KDG vor?
- Gibt es stattdessen ausreichende Garantien im Sinne des § 40 Abs. 2 KDG?
- Ist nach § 41 KDG ausnahmsweise die Zulässigkeit der Übertragung in das Ausland gegeben?

Für den gesamten Bereich des Auslandsbezuges muss der übermittelnden Dienststelle auch klar sein, dass sie als Behörde des öffentlichen Rechts tätig wird. Soweit sich Ausnahmen für die Übermittlungsbefugnis aus zwischenstaatlichen handelsrechtlichen Verträgen ergeben, reicht dies normalerweise noch nicht für eine Mitteilung durch eine Behörde, sofern die übrigen Voraussetzungen des § 40 KDG nicht gegeben sind.

Die Einwilligung

Alle Rechtsnormen über den Datenschutz sehen vor, dass auch bei Fehlen einer gesetzlichen Grundlage die Datenverarbeitung jedenfalls dann zulässig ist, wenn der Betroffene einwilligt. Die Prüfung einer Einwilligung ist aber gegenüber derjenigen einer Aufgabe sekundär und nur notwendig, wenn es an einer Aufgabe fehlt!

Eine Einwilligung ist auch nur dann wirksam, wenn der Betroffene auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie – auf Verlangen – auf die Folgen der Verweigerung der Einwilligung hingewiesen wird. Die Einwilligung bedarf der Schriftform und muss klar als solche erkennbar sein (§ 8 Abs.2 KDG). Die Einwilligung muss auf Freiwilligkeit beruhen (§ 8 Abs. 1 Satz 2 KDG). Wird von einem Betroffenen eine Einwilligung verlangt, sollte darauf hingewiesen werden, dass die Ablehnung dieses Ansinnens keine Nachteile für ihn bringt.

Einwilligungen spielen vor allem eine Rolle, wenn es um die **Veröffentlichung von personenbezogenen Daten** geht. Hier kann unter Umständen auch die Art der Veröffentlichung eine Rolle spielen: Die Nennung im Internet hat viel

weitergehende Auswirkungen als zum Beispiel die Nennung in einem Lokalblatt. Eine Besonderheit im kirchlichen Bereich stellt der

Pfarrbrief

dar. Er war ursprünglich nichts weiter als eine Mitteilung an die Mitglieder der Kirche und als solcher keine Mitteilung an Dritte im Sinne des § 10 KDG. Diese Überlegung folgte daraus, dass der Pfarrbrief eigentlich nur eine schriftliche Mitteilung wie alle übrigen Briefe darstellt. Die rechtliche Beurteilung hat sich inzwischen aber geändert, weil Pfarrbriefe

- auch an Nichtmitglieder verteilt
- außerhalb der Kirche ausgehängt
- im Internet veröffentlicht oder
- an die Presse weitergeleitet werden.

Liegt einer dieser Fälle vor, so ist eine Nennung personenbezogener Daten im Pfarrbrief eine Mitteilung auch an Dritte. Das ist häufig bedeutsam, wenn im Pfarrbrief Jubiläen (Geburtstag, Silberhochzeit usw.), Sakramentenspendung (Taufe, Eheschließung, Erstkommunion, Firmung) oder die Stiftung von Messen erwähnt werden. Bei der Messstiftung ist allerdings nur die Nennung des (lebenden) Stifters, nicht die des Verstorbenen, für den die Messe gelesen wird, von Bedeutung. Der Verstorbene selbst genießt keinen Datenschutz. Da es keine kirchliche Aufgabe für die Veröffentlichung der bezeichneten Vorgänge gibt, ist ihre Nennung im Pfarrbrief dann bedenklich, wenn eine der oben genannten Voraussetzungen vorliegt. Es bedarf dann einer Einwilligung des Betroffenen in Schriftform.

Eine Sonderform der Übermittlung: Datenverarbeitung im Auftrag, § 26 KDG

Viele kirchliche Dienststellen lassen ihre Daten durch einen externen Datenverarbeiter aufbereiten. Der Markt für derartiges „Outsourcing“ wächst ständig. Im Prinzip macht durch eine derartige vertragliche Auslagerung der Datenverarbeitung die kirchliche Dienststelle eine Datenübertragung an ein gewerbliches Unternehmen. Das ist auch im staatlichen Bereich sehr häufig und deswegen ebenso im Bundesdatenschutzgesetz geregelt. Wichtig bei derartigen Vorgängen ist die Einhaltung von § 29 Abs. 4 KDG. Die dort normierten Mindestanforderungen an den Vertrag gewährleisten, dass die kirchliche Dienststelle als Auftraggeber dem Auftragnehmer gegenüber die Rechte hat, die sie benötigt, um ihrerseits den Vorwurf fehlerhafter Datenbehandlung abzuwehren. Nach Abs. 4 der Vorschrift gilt diese nicht nur für die externe Datenverarbeitung, sondern auch für Fernwartungsverträge. Muster für diese Vertragsgestaltung finden Sie auf der Downloadseite.

Noch ein Hinweis: Das KDG spricht an mehreren Stellen von dem Auftragsverarbeiter und folgte damit der Linie der EU-DS-GVO. Wenn man das so liest, könnte man die Auffassungen gewinnen, damit sei auch der externe Auftragsverarbeiter – also zum Beispiel das Unternehmen, das für eine kirchliche Dienststelle die Speicherung auf seinen Rechnern vornimmt – gemeint. Man käme dann dazu, anzunehmen, dass auch für dieses externe Unternehmen das KDG direkt gilt. Dem ist aber nicht so: Man kann sich nicht einfach die Rechtsordnung heraussuchen, unter die man fallen will. Das KDG gilt nur für kirchliche Dienststellen. Es kann auch nicht im Wege der Vertragsgestaltung zur herrschenden Rechtsordnung gemacht werden, weil man - wie gesagt - sich die Rechtsordnung nicht heraussuchen kann, unter die man fallen will. Ist daher die Geltung von Vorschriften des KDG im Vertrag zwischen der kirchlichen Dienststelle und dem externen Auftragsverarbeiter vereinbart, so ergibt sich daraus nur ein schuldrechtlicher Anspruch gegen den Auftragsverarbeiter. Der Auftragsverarbeiter unterliegt als Externer immer direkt der EU-DS-GVO. Was das KDG mit dem Begriff Auftragsverarbeiter meint, ist klar: einzig und allein den kirchlichen Datenverarbeiter wie zum Beispiel das kirchliche Rechenzentrum, das für ein Bistum die Lohnbuchhaltung übernommen hat. Auch dieser Vertrag unterliegt natürlich den Anforderungen des § 29 KDG.

Löschung von Daten

Die von kirchlichen Dienststellen erhobenen und noch gespeicherten Daten sind spätestens dann zu löschen, wenn sie nicht mehr benötigt werden. War ihre Speicherung von Anfang an unzulässig, sind sie sofort zu löschen (§ 19 Abs. 1 a KDG). Das Problem dabei ist, dass die gespeicherten Daten nicht von sich aus auf ihre Löschungsbedürftigkeit aufmerksam machen. Hinzu kommt, dass der Festplattenspeicher inzwischen derart billig ist und kaum eine Dienststelle von sich aus auf die Löschung hinwirken will. Bei neu zu entwickelnden Programmen ist es deshalb zweckmäßig, Löschungs– oder Erinnerungsroutinen einzubauen, die in regelmäßigen Abständen den Nutzer auf die Notwendigkeit der Löschung überflüssiger Daten hinweisen.

Die **Löschung** muss wirklich **verhindern**, dass ausgesonderte Daten später wieder hergestellt werden. Bei papiergebundenen Daten sollte der Reißwolf benutzt werden und mindestens der Schutzklasse drei angehören. Bei Computerdaten ist zu berücksichtigen, dass die Löschung lediglich den Eintrag der Datei im Inhaltsverzeichnis des Rechners beseitigt, die Daten als solche aber unangetastet lässt. Sie sind nur dann nicht wieder herstellbar, wenn sie – möglichst mehrfach – überschrieben werden. Dazu gibt es für die meisten Fälle völlig ausreichende Freewareprogramme.

Eine etwas merkwürdig anmutende Regelung ist darin zu sehen, dass auch zu löschende Daten zunächst **nach der kirchlichen Archivordnung dem Archiv angeboten** werden müssen. Wenn das Archiv sie übernimmt, so gelten die Daten im Rechtssinne als gelöscht, obwohl sie unter Umständen für sehr lange Zeit aufbewahrt werden. Man spricht in diesem Zusammenhang von einem Löschungssurrogat. Dieses Löschungssurrogat ist besonders wichtig bei Datenspeicherungen, die von vornherein unzulässig waren. Würde nämlich tatsächlich in diesen Fällen eine Löschung stattfinden, so wäre dem Betroffenen der Nachweis unmöglich, dass eine unzulässige Datenspeicherung stattgefunden hat.

Nicht gelöscht werden dürfen Daten, für die es gesetzliche Aufbewahrungsfristen gibt, § 19 Abs. 3 Buchst. b KDG. Eine Zusammenstellung gesetzlicher Aufbewahrungsfristen von Sozialdaten finden Sie im Internet.

Auskunft

Das Gegenstück zum Recht der Dienststelle auf Speicherung der Daten von Betroffenen ist deren Auskunftsrecht nach § 17 KDG. Die Auskunft wird in aller Regel durch Übergabe einer Kopie der gespeicherten Aktenstücke oder durch Akteneinsicht erteilt, nur ausnahmsweise mündlich. Für einen Antrag auf Auskunft gibt es keine bestimmten Formvoraussetzungen; der Antrag soll nur die Art der Daten bezeichnen, zu denen Auskunft begehrt wird. Gerade bei der Auskunftsverpflichtung empfiehlt es sich, die Rechte der Betroffenen sehr ernst zu nehmen. Verlangt nämlich ein Betroffener formell Auskunft, so fühlt er sich meistens schon in seinen Rechten verletzt. Es sollte ihm kein Anlass gegeben werden, das bestätigt zu sehen.

Das KDG hat darüber hinaus für all die Fälle, in denen Daten ohne Wissen des Betroffenen erhoben wurden, auch eine Informationspflicht geschaffen: Nach § 15 ist der Betroffene darüber zu informieren, dass seine personenbezogenen Daten erhoben wurden, wenn er darüber nicht ohnehin schon Bescheid weiß (Abs. 4). Dies kommt vor allem bei der datenbankmäßigen Erfassung von Spendern in Betracht.

Noch weitergehend: Jeder, dessen Daten irgendwann in einer Datenbank gelandet sind, kann verlangen, dass sie aus dieser auch gelöscht werden, zum Beispiel, wenn er seine Einwilligung zur Datenspeicherung widerruft. In einem solchen Fall ist unverzüglich zu löschen, § 19 KDG. Statt der Löschung kann bei den Inhalten einer Datenbank auch verlangt werden, dass sie einem anderen Verantwortlichen übertragen werden.

Wenn eine Datenschutzverletzung geschehen ist, so kann daraus ein ganz erheblicher Schaden resultieren. Um ihn möglichst klein zu halten, schrieb schon bisher das BDSG vor, was zu tun ist. Dies ist inzwischen mit § 33 KDG auch in dieses übernommen worden. Erwächst also aus dem Vorliegen einer Datenschutzverletzung einer Person ein Risiko für ihre Rechte, so ist sofort die Datenschutzaufsicht zu verständigen. Sie verfügt, was weiter zu geschehen hat.

Besonderheiten des Mitarbeiterdatenschutzes

Der Mitarbeiterdatenschutz ist sowohl im Bundesdatenschutzgesetz wie auch im Kirchlichen Datenschutzgesetz eher stiefmütterlich behandelt. Das liegt daran, dass schon vor dem ersten Inkrafttreten des Bundesdatenschutzgesetzes 1983 die Rechtsprechung des Bundesarbeitsgerichtes den Arbeitnehmern bestimmte Datenschutzrechte sicherte. Als es dann in das BDSG eingefügt wurde, bildete die Vorschrift nur einen Teil des Richterrechts ab. Es gab 2013 einen großen Entwurf für eine entsprechende Erweiterung des Mitarbeiterdatenschutzes im BDSG; dieser wurde jedoch nie Gesetz. § 53 KDG entspricht im Wortlaut fast vollständig dem § 26 BDSG; lediglich die Worte“ einschließlich der religiösen Überzeugung“ fehlen im Gesetz. Über diese gesetzliche Regelung hinaus gibt es eine ganze Reihe von Regelungen, die auf gerichtlichen Entscheidungen beruhen und im Ergebnis auch auf das für die Mitarbeiter der katholischen Kirche maßgebliche Arbeitsrecht anwendbar sind:

- Alle Daten müssen grundsätzlich beim Mitarbeiter erhoben werden.
- Der Dienstgeber darf nur solche Daten erheben, die zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder gesetzlich vorgesehen sind.
- Der Grundsatz der Zweckbindung ist streng zu beachten.
- Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Mitarbeiters führen kann, ist unzulässig.
- Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden. Dies wird durch § 24 KDG noch einmal stark verdeutlicht. In den Fällen des sogenannten „Profiling“ werden die Beurteilung erheblicher Tatsachen allein aus automatisiert erhobenen Daten gewonnen, vgl. § 4 Abs. 5 KDG.
- Dem Dienstgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung bekannt gegeben werden.
- Den Mitarbeitern sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die ihr Arbeitsverhältnis betreffen.

Der Zugriff auf Mitarbeiterdaten unterliegt ebenfalls strenger Zweckbindung. So können zum Beispiel Daten, die der Dienstgeber für die Sozialversicherung erhoben hat, nur für diesen Zweck verwendet werden. Eine Einwilligung des Mitarbeiters kommt als Rechtfertigung und Grundlage einer Datenerhebung oder Datenverarbeitung nur dann infrage, wenn die Freiwilligkeit der Einwilligung sichergestellt ist.

Schadensersatz und Geldbußen

Bisher war es so, dass Verantwortliche für schuldhaft herbeigeführte Datenschutzverletzungen Schadensersatz leisten mussten. Der Anspruchsteller war verantwortlich dafür, die Tatsache der Datenschutzverletzung und das Verschulden nachzuweisen. Das Bundesdatenschutzgesetz und das Datenschutzrecht der EKD hatten eine andere Regelung: der Verantwortliche haftete nur dann, wenn er nicht beweisen konnte, dass ihn kein Verschulden traf. Diese Regelung hat in § 50 Abs. 3 das KDG auch übernommen.

Ganz neu ist die von der EU-DS-GVO vorgegebene Einführung von Geldbußen für die schuldhafte Herbeiführung von Datenschutzverletzungen. Dabei wird gegen Dienststellen der verfassten Kirche nach § 51 Abs. 6 KDG keine Geldbuße verhängt, sondern nur gegen deren Verantwortliche. Zuständige Geldbußenbehörde ist die Datenschutzaufsicht. Sie bemisst die Geldbuße nach § 51 Abs. 3 KDG. Wenn der Betroffene sich nicht dagegen wendet, wird die Geldbußenforderung bei ihm vollstreckt. Er kann sich aber auch an das Datenschutzgericht wenden und in diesem Verfahren die Tatbestandsmäßigkeit in Frage stellen. Verfahrensordnung ist dann diejenige des Datenschutzgerichts. Greift der Betroffene die Höhe der Geldbuße an, geht das Verfahren an das staatliche Amtsgericht; Verfahrensordnung ist das Ordnungswidrigkeitengesetz.

Exkurs 1: Videoüberwachung

Wie schon oben dargestellt, wird die Videoüberwachung in dem KDG aus Gründen des Zusammenhangs in § 52 KDG mit geregelt, weil die Videoüberwachung eigentlich Bilder und nicht personenbezogene Daten erfasst. Eine zulässige Videoüberwachung setzt dreierlei voraus:

- Eine Beobachtung durch eine Videoanlage darf nur stattfinden, wenn es einen Grund hierfür gibt und die schutzwürdigen Interessen der Betroffenen nicht überwiegen. Grund ist in der Regel die Wahrnehmung des Hausrechts und der Schutz von Gebäuden oder beweglichen Sachen vor Diebstahl oder Beschädigung. Das KDG verlangt ebenso wenig wie das BDSG einen vorangegangenen Vorfall, der die Befürchtung einer Rechtsverletzung wahrscheinlich werden lässt. Es dürfen nur nicht die schutzwürdigen Interessen der beobachteten Betroffenen überwiegen. Von mehreren Diözesandatenschutzbeauftragten in Deutschland wird die Auffassung vertreten, dass Innenräume von Kirchen, die zum Gebet genutzt werden, grundsätzlich nicht vollständig überwacht werden dürften. Dieser Auffassung folge ich nicht; insbesondere darüber nicht ohnehin schon Bescheid weiß (Abs. 4) Insbesondere findet die Annahme, für eine Teilüberwachung einer Kirche müssten gravierende Gründe benannt werden, keine Stütze im Gesetz. Dass während der Heiligen Messe die Videoüberwachung abgeschaltet sein muss, versteht sich von selbst. Im Übrigen ist die rein tatsächliche Folge fehlender Videoüberwachung regelmäßig die Schließung der Kirche außerhalb der Messzeiten, auch wenn dies so nicht sein dürfte.
  Da die Auswirkungen einer Videoattrappe denjenigen einer tatsächlich vorhandenen Videokamera entsprechen, bedarf es auch für die Anbringung einer Attrappe eines entsprechenden Bedürfnisses und seiner Feststellung. Natürlich muss kein Hinweis auf die Attrappe angebracht werden, da der Hinweis „Vorsicht Attrappe“ wenig hilfreich und ein Hinweis auf eine tatsächlich vorhandene Videokamera wahrheitswidrig wäre.
  In der Praxis entscheidet der Kirchenverwaltungsvorstand durch Beschluss, der in der üblichen Weise bekannt gemacht wird, und setzt anschließend diesen Beschluss in die Praxis um. Eine zentrale Erfassung aller Videoüberwachungen ist nicht geboten.
- Auf die Tatsache der Videoüberwachung muss durch geeignete Maßnahmen – in der Regel durch ein Hinweisschild – hingewiesen werden, § 52 Abs. 2 KDG.
- Die erhobenen Videobilder oder Filme sind regelmäßig zu löschen, wenn sie nicht zu Beweiszwecken benötigt werden. Zweckmäßigerweise wird der vorhandene Speicher in regelmäßigen Abständen überschrieben.

Exkurs 2: Bilder und Filme

Das Inkrafttreten der Europäischen Datenschutz-Grundverordnung ab dem 25.5.2018 hat viele Dienststellenleitungen zu Recht dazu gebracht, das bisherige Vorgehen im Zusammenhang mit der Anfertigung und Veröffentlichung von Bildmaterial auf seine Rechtmäßigkeit zu überprüfen. Dabei war es noch nicht einmal diese Gesetzesänderung, die den großen Einschnitt bewirkte, sondern ein Urteil des Europäischen Gerichtshofs aus dem Jahre 2014[4], in welchem das Fertigen eines digitalen Fotos, mithilfe dessen man die fotografierte Person identifizieren konnte, schon als Erhebung personenbezogener Daten gesehen wurde. Diese Wegweisung des Europäischen Gerichtshofs musste natürlich unter dem Gesichtspunkt der neuen Rechtslage ihre Auswirkung haben.

Zum Vergleich: Bisher war nur die Verbreitung von Fotografien – analogen wie digitalen – durch §§ 22ff.

[4] ZD 2015, 77

Kunsturhebergesetz (KUG) vom 9.1.1907 geregelt und eingeschränkt worden.

Ausgangspunkt ist § 22 Kunsturhebergesetz:

§ 22 [Recht am eigenen Bilde]

[1]Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. [2]Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt. [3]Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. [4]Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten, und wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.

Bildnisse in diesem Sinne sind nicht nur Fotografien, sondern auch Filme**. Verbreiten** ist nicht nur die Weitergabe von Papierabzügen, sondern auch diejenige von digitalen Kopien, zum Beispiel auf CD-ROMs. **Zurschaustellen** ist immer dann gegeben, wenn eine unkontrollierbare Öffentlichkeit Kenntnis von dem Bild oder dem Film nehmen kann. Auch das Zeigen von Bildern innerhalb eines nicht geschlossenen Personenkreises, zum Beispiel Arbeitskollegen, kann den Tatbestand erfüllen. Die **Vervielfältigung** ist ein den anderen vorgelagerter Sachverhalt, also eigentlich eine Versuchshandlung.

Die Konsequenz aus dieser Vorschrift ist, dass die Veröffentlichung oder das Zurschaustellen von Bildern ohne die erforderliche Einwilligung rechtswidrig und sogar eine Straftat nach § 30 Kunsturhebergesetz ist. Zu beachten ist auch, dass anders als im engeren Datenschutzrecht das Recht am eigenen Bild über den Tod hinaus besteht. Für einen Zeitraum von 10 Jahren sind die näheren Angehörigen verfügungsbefugt.

Alles, was das KUG bei der Verbreitung erlaubte, war früher natürlich bei der Fertigung der Aufnahme ebenfalls erlaubt – oder einfach nicht geregelt. Im Hinblick auf das zitierte Urteil des EuGH wurde aber bald diskutiert, ob nicht das Fertigen eines Fotos nach den neuen Regelungen zum Datenschutz separat zu bewerten sei. Da bereits die Fertigung des Bildes oder Films als Datenverarbeitung anzusehen ist, bedarf es dafür einer – weiteren - Rechtsgrundlage. Zieht man eine Einwilligung als Rechtfertigung heran, bedarf es streng genommen zweier:

- derjenigen für die Aufnahme und
- derjenigen für die Verbreitung.

Angesichts des Umstandes, dass § 8 Abs. 2 KDG in der Regel für die Erlaubnis eine Schriftform verlangte, war die Bürokratisierung aller Fotografie vorprogrammiert: Man stelle sich ein Schulfest vor, bei dem der Vertrauenslehrer vor Fertigung der Fotografien zunächst die schriftlichen Einwilligungen zur Aufnahme seitens der Eltern einholte,, dann die Bilder ausdruckte, den Eltern der auf ihnen abgebildeten Kinder zur Genehmigung vorlegte und sie schließlich verbreitete. Mittlerweile hat sich die Diskussion etwas abgekühlt. Das Kopfnicken der abzubildenden Erwachsenen oder das Passieren einer entsprechenden Hinweistafel wird als ausreichendes Einverständnis mit dem fertigen der Aufnahme angesehen. Bei Eltern ist es erforderlich, dass sie vorweg ihre Einwilligung erklärt haben. Die Verbreitung richtet sich dann wieder nach dem Kunsturhebergesetz. Von dessen Vorschrift des § 22 gibt es Ausnahmen:

§ 23 [Ausnahmen zu § 22]
(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:
1. Bildnisse aus dem Bereiche der Zeitgeschichte;
2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;
4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.
(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

Für den kirchlichen Bereich am bedeutsamsten ist die Ausnahme in Absatz 1 Nummer 3. Die hier verwendeten Begriffe „Versammlung“ und „Aufzug“ sind sehr weit auszulegen. Hierunter werden alle Ansammlungen von Men-

schen, die den kollektiven Willen haben, etwas gemeinsam zu tun, verstanden (so OLG München NJW 1988, 915). Dazu gehören zum Beispiel Menschenansammlungen, Sportveranstaltungen, Kongresse, Vereinsveranstaltungen, Hochzeitsgesellschaften und Beerdigungen. Die Erkennbarkeit einzelner schließt die Rechtfertigung nach dieser Vorschrift nicht aus. Es muss jedoch die Versammlung im Vordergrund stehen und nicht die Abbildung einzelner Menschen. Andererseits kommt es nicht darauf an, dass die gesamte Veranstaltung abgebildet ist, da die Rechtfertigung auch für repräsentative Teilausschnitte gilt.

Um im kirchlichen Bereich möglichst klare Regeln zu haben, gab ich als Anhaltspunkte für die Beurteilung:

- Auf dem Bild müssen mindestens 8 Personen abgebildet sein.
- Es darf sich nicht um eine gestellte Aufnahme handeln.

Wenn keine der in § 23 genannten Ausnahmen vorliegt, bedarf jede Veröffentlichung der **Einwilligung der abgebildeten Person**, bei Minderjährigen der Einwilligung aller Sorgeberechtigten. Die Einwilligung kann auch für **künftige Abbildungen** erklärt werden, ist jedoch frei widerrufbar für diejenigen Bilder, die nach dem Widerruf veröffentlicht werden sollen. In der Downloadseite finden sich entsprechende Muster, die natürlich – wie alle Muster – im Wortlaut abgeändert werden können, sofern dadurch keine Änderung im Sinn eintritt.

Die Datenschutzbeauftragten

Das KDG kennt zwei Datenschutzbeauftragte, den Diözesandatenschutzbeauftragten als Leiter der Datenschutzaufsicht nach § 42 bzw. bei Ordensgemeinschaften den Ordensdatenschutzbeauftragten und den betrieblichen Datenschutzbeauftragten nach § 36.

Der Diözesan- oder Ordensdatenschutzbeauftragte

Sie stehen rechtlich gleich, weil nach dem Kirchenrecht ein Orden päpstlichen Rechts einem Bistum gleichgesetzt wird. Bei Orden bischöflichen Rechts ist der Diözesandatenschutzbeauftragte zuständig. Um im Folgenden Wiederholungen zu vermeiden, werden die Ausführungen nur auf den Diözesandatenschutzbeauftragten gemünzt; sie gelten in gleicher Weise für den Ordensdatenschutzbeauftragten. Abweichungen hebe ich hervor.

Der Diözesandatenschutzbeauftragte ist die obere, vom Diözesanbischof (bzw. Ordensoberen) berufene Datenschutzinstanz. Das KDG sieht ausdrücklich vor, dass ein Diözesandatenschutzbeauftragter für mehrere Diözesen bestellt werden kann (§ 42 Abs. 1 Satz 3 KDG). Der Diözesandatenschutzbeauftragte soll Volljurist sein und völlig unabhängig von der Kirche. Er darf also nicht kirchlicher Bediensteter im Hauptamt und Datenschutzbeauftragter im Nebenamt oder umgekehrt sein.

Die Bestellung des Diözesandatenschutzbeauftragten erfolgt für mindestens vier und höchstens acht Jahre. Eine vorzeitige Abberufung ist nur unter engen Voraussetzungen möglich; allerdings kann der Diözesandatenschutzbeauftragte sein Amt vorzeitig zurückgeben. Im Verhältnis zu den kirchlichen Dienststellen hat er ein Weisungsrecht (vgl. § 44 Abs. 2 a KDG). Er berät die kirchlichen Dienststellen im Hinblick auf den Datenschutz und spricht dabei Empfehlungen aus.

Im staatlichen Recht würde seine Stellung derjenigen des Bundesdatenschutzbeauftragten bzw. des Landesdatenschutzbeauftragten entsprechen. Demnach wacht der Diözesandatenschutzbeauftragte über die Einhaltung der kirchlichen Datenschutzordnung sowie der anderen kirchlichen und staatlichen Vorschriften über den Datenschutz in seinem Bereich. Jedermann kann ihn gemäß § 48 KDG anrufen, wenn er sich in seinen Datenschutzrechten verletzt fühlt. Insofern hat der Diözesandatenschutzbeauftragte eine gerichtsähnliche Funktion (vgl. auch § 48 Abs. 4 KDG). Stellt der Diözesandatenschutzbeauftragte nach Prüfung des Sachverhalts (§ 48 Abs. 2 KDG) oder aufgrund seiner

Kontrollen Verstöße gegen Datenschutzvorschriften fest, so beanstandet er das Vorgehen der kirchlichen Dienststelle und fordert die Dienststelle unter Fristsetzung zur Behebung auf (§47 Abs. 1 KDG).

Der Diözesandatenschutzbeauftragte ist nach dem Urteil des europäischen Gerichtshofs vom 9.3.2010 verpflichtet, die Einhaltung des Datenschutzes in den kirchlichen Dienststellen durch Kontrollen zu überprüfen. Dazu steht ihm nach § 43 Abs. 4 und 5 eine angemessene Personalausstattung zu. Das Personal wird zwar von einer kirchlichen Stelle angestellt, doch untersteht es der ausschließlichen Weisungsbefugnis des Diözesandatenschutzbeauftragten.

Der betriebliche Datenschutzbeauftragte

Grundsätzliches

Während in anderen europäischen Ländern wie zum Beispiel Frankreich die Datenschutzaufsicht zentral geregelt ist, baut Deutschland entsprechend seiner föderalen Struktur auf den Grundsatz, dass die Aufsichtsaufgaben überwiegend möglichst sachnah angesiedelt werden. Deswegen kennen alle deutschen Datenschutzordnungen einen behördlichen oder betrieblichen Datenschutzbeauftragten. Ohne diesen wäre die Aufgabe des Diözesandatenschutzbeauftragten fast unmöglich zu bewerkstelligen. Der betriebliche Datenschutzbeauftragte ist demnach eine von der jeweiligen kirchlichen Dienststelle bestimmte oder eingesetzte Person, die für eine oder mehrere Einrichtungen der Dienststelle den Datenschutz fördert. Das kann sowohl durch Kontrollen wie auch durch Beratung oder durch die Abhaltung von Fortbildungsmaßnahmen geschehen.

Nach § 36 Abs. 1 KDG benennen kirchliche Dienststellen der verfassten Kirche immer einen betrieblichen Beauftragte für den Datenschutz und zeigen dies dem Diözesandatenschutzbeauftragten an (Abs. 4 S.2).

Der betriebliche Datenschutzbeauftragte entlastet den Dienststellenleiter ganz erheblich. Soweit der Dienststellenleiter zur Erstellung eines Datenschutzkonzepts verpflichtet ist, bereitet der betriebliche Datenschutzbeauftragte dies vor und bespricht es mit dem Dienststellenleiter. Im Übrigen fördert der betriebliche Datenschutzbeauftragte die Motivation der Mitarbeiter im Hinblick auf den Datenschutz und deren Fortbildung.

Der betriebliche Datenschutzbeauftragte kann ein interner (Mitarbeiter) oder externer (Beauftragter, häufig ein Rechtsanwalt) sein. Vor allem bei kleineren Dienststellen ist häufig ein Mitarbeiter eingesetzt, der eine gewisse Stundenermäßigung für seine übrigen Tätigkeiten erhält.

Bestellung

Zum betrieblichen Beauftragten für den Datenschutz darf nur bestellt werden, wer die erforderliche „Fachkunde und Zuverlässigkeit“ besitzt. Der betriebliche Datenschutzbeauftragte muss also sowohl die technische als auch die rechtliche Seite seiner Aufgaben kennen und Kenntnisse in allen Bereichen haben, die für die Organisation, in der er arbeitet, von Bedeutung sind. Aber: Es ist realistisch, die Anforderungen nicht zu hoch anzusetzen. Im Zweifel ist es besser, überhaupt einen betrieblichen Datenschutzbeauftragten zu haben! Da gerade für den internen betrieblichen Datenschutzbeauftragten eine längere Abwesenheit zum Zwecke der Fortbildung schlecht verkraftbar ist, muss auch darauf gesetzt werden, dass er sich selbst nach einer Einführungsveranstaltung mit schriftlichem Material aus- und fortbildet

Der Dienststellenleiter – bei Ordensgemeinschaften der Ordensobere – bestellt den betrieblichen Datenschutzbeauftragten durch schriftliche Anordnung. Wird – wie häufig – für den Bereich eines Dekanats ein gemeinsamer betrieblicher Datenschutzbeauftragter bestellt, so muss die Bestellung von allen Pfarrern der einzelnen Kirchenstiftungen unterzeichnet werden. Hierfür gibt es ein entsprechendes Formblatt in der Downloadseite.

Rechtsstellung

Der interne betriebliche Datenschutzbeauftragte ist dem Dienststellenleiter bzw. dem Leiter einer selbständigen Einrichtung unmittelbar zu unterstellen. Um seine Unabhängigkeit in der Wahrnehmung seiner fachlichen Aufgaben

zu gewährleisten, bestimmt das KDG, dass er in der Ausübung seiner Fachkunde weisungsfrei ist (§ 3 Abs. 1 S. 2). Niemand – auch nicht der Leiter der Dienststelle – kann vorschreiben, wie er datenschutzrechtliche Fragen zu bewerten hat. Dazu kommt eine Auswirkung auf ein eventuelles Arbeitsverhältnis des betrieblichen Datenschutzbeauftragten. Er genießt Kündigungsschutz wie ein Mitglied der Mitarbeitervertretung.

Wenn sich der Dienststellenleiter über das Votum des betrieblichen Datenschutzbeauftragten hinwegsetzt, weil er selbst in letzter Konsequenz die Verantwortung für die Daten verarbeitende Stelle trägt, kann sich der betriebliche Datenschutzbeauftragte an den Diözesandatenschutzbeauftragten wenden. Ganz generell ist überhaupt der betriebliche Auge und Ohr des Diözesandatenschutzbeauftragten. Der Diözesandatenschutzbeauftragte wendet sich zum Beispiel seinerseits bei Beschwerden über eine Einrichtung immer erst an dem betrieblichen, bittet ihn um Sachverhaltsaufklärung und hört ihn an. Umgekehrt versorgt der Diözesandatenschutzbeauftragte den betrieblichen mit den notwendigen Informationen und ist immer für ihn zu sprechen.

Eines ist nach Auffassung aller Diözesan- und Ordensdatenschutzbeauftragten sicher: Der betriebliche Datenschutzbeauftragte haftet nicht für Datenschutzverletzungen, die er nicht böswillig herbeigeführt hat[5].

Das Verfahren vor dem Datenschutzgericht

Anlass für entsprechende Überlegungen

Art. 91 der EU-Datenschutz Grundverordnung stellt die Kirchen und religiösen Vereinigungen den Staaten gleich. In Art. 77ff. wiederum ist geregelt, dass es einen wirksamen Rechtsbehelf gegen Entscheidungen der Aufsichtsbehörde ebenso wie gegen die Verantwortlichen geben muss. Derartiges fehlt in der bisherigen kirchlichen Datenschutzordnung.

Es musste demnach geprüft werden, ob ein Rechtsbehelfsverfahren gegen Entscheidungen der Aufsichtsbehörde bzw. den Verantwortlichen zu den unverzichtbaren Voraussetzungen eines eigenen kirchlichen Datenschutzes – und damit der kirchlichen Selbstverwaltungsfreiheit – gehört. Das ist dann der Fall, wenn ohne eine derartige Regelung die Gleichwertigkeit nicht gewährleistet wäre. Bei dieser Gelegenheit bietet es sich natürlich an, zu fragen, warum man nicht einfach den Rechtsweg den staatlichen Gerichten der Bundesrepublik überlässt. Dies würde es allen Religionsgemeinschaften in Deutschland ermöglichen, darauf zu verzichten. Die ganz andere Frage ist jedoch, ob bei einer solchen Regelung die Selbstverwaltungsfreiheit noch gewahrt wäre. Anders herum: Können staatliche Gerichte über Datenschutzfragen einer Organisation entscheiden, ohne dass die Selbstverwaltungsfreiheit dieser Organisation beeinträchtigt wird. Die Frage stellen heißt sie verneinen: Es ist nicht möglich, Datenschutzinterna auf ihre Rechtmäßigkeit zu überprüfen, ohne „in das Eingemachte" zu gehen, d.h. zu prüfen, was legal und was illegal ist. Also musste erwogen werden, eine eigene Verfahrensordnung hierfür aufzubauen.

Die kirchlichen Gremien, welche sich mit den Rechtsetzungsvorschlägen befassen, waren im letzten Jahr und sind immer noch mehr als gut ausgelastet. Hätte es sich da nicht angeboten, einfach die staatliche Verwaltungsgerichtsordnung abzuschreiben oder gar nur auf sie Bezug zu nehmen, um sich viel Gesetzgebungsarbeit zu sparen? Die VwGO umfasst 195 Paragrafen – viele von ihnen regeln Formalia, Fristen, Zuständigkeiten. Gerade diese Dinge erwartet man nicht unbedingt in einer kirchlichen Verfahrensordnung. Sie würden auch in der Praxis zu ganz erheblichen Erschwernissen führen, weil der Blick abgelenkt wird von der Berechtigung eines Anliegens zur formalen Rechtsposition. Hinzu kommt, dass all diese Formalia in ihrer praktischen Umsetzung dazu führen würden, eine Unmenge neuer Dienststellen zu schaffen, juristisch auszustatten und ständig in der Umsetzung zu kontrollieren. Und es gibt noch ein Problem, speziell der katholischen Kirche: Wir haben nie verschwiegen, dass wir aus historischen

[5] https://www.erzbistum-muenchen.de/cms-media/media-42923320.pdf

Gründen keine demokratische Grundordnung haben, d. h. unser Diözesanbischof ist Legislative, Exekutive und Judikative in einer Person. Wenn wir nun den 27 Bischöfen in Deutschland vorschlagen würden, je ein Werk von ca. 100 Druckseiten in Kraft zu setzen, käme ganz zu Recht die Frage zurück, ob wir das müssen, ob wir einander so wenig trauen, dass so viel geregelt werden muss. Und so wurde allmählich die Frage „Braucht es das wirklich?" zum ständigen Begleiter derjenigen, die sich mit dem Entwurf der Verfahrensordnung herumschlugen. Normalerweise dürfen wir uns die Frage gar nicht stellen, weil der Bundes- oder Landesgesetzgeber sie für uns abschließend beantwortet hat. So kommt es, dass auch die Vorbereitung innerkirchlicher Gesetze nicht ohne ihre charmanten Seiten ist.

Das Grundkonzept

Zunächst bedarf es eines Trägers für eine Gerichtsbarkeit; in der Bundesrepublik sind das der Bund und Länder. Hier zeigen sich schon die ersten Schwierigkeiten: Es gibt keine einheitliche katholische Kirche in Deutschland - da haben uns die Freunde von der EKD einiges voraus. Die deutsche katholische Kirche ist in Diözesen und - um es noch etwas komplizierter zu machen - in Ordensgemeinschaften päpstlichen Rechts gegliedert. Diese Ordensgemeinschaften stehen den Bistümern auch in der Gesetzgebungsbefugnis gleich. Selbstverständlich müssen sie in die Verfahrensordnung eingebunden sein, weil diese ja nicht nur für die verfasste Kirche, sondern auch für die Orden gelten soll.

Da es keine institutionelle und hergebrachte überörtliche gemeinsame Institution der katholischen Kirche in Deutschland gibt, muss auf den Verband der Diözesen Deutschlands (VDD) als Träger zurückgegriffen werden. Der Verband hat seinen Sitz in Bonn und dort wird auch der erste Sitz des kirchlichen Datenschutzgerichtes zweiter Instanz sein; das der ersten Instanz in Köln. Natürlich muss dieses Datenschutzgericht alle Anforderungen erfüllen, die in einem Rechtsstaat an es gestellt werden. Das bedeutet

- einfacher Zugang für jeden Betroffenen ohne unnötige formale Hürden
- klare Zuständigkeitsregelungen
- Verankerung des rechtlichen Gehörs
- rechtsstaatliches Verfahren
- Außenwirkung der Entscheidung
- Möglichkeit eines Rechtsbehelfs.

Von vorneherein erschien es ausreichend, für das Datenschutzverfahren zwei Instanzen vorzusehen. Sie bieten ausreichend Gelegenheit, ein Vorbringen auf seine Stichhaltigkeit zu prüfen. Auch im internationalen Vergleich sind zwei Instanzen ein guter Mittelwert; wir müssen nicht in allen Fällen eine Tatsachen- und eine gesonderte Rechtsinstanz vorsehen. Zumindest in den ersten zehn Jahren wird sich die Belastung des Gerichts wohl in Grenzen halten. Deswegen erschien es sinnvoll, die beiden für das Gericht vorgesehenen Instanzen in einem Gerichtskörper mit einem gemeinsamen Präsidenten anzusiedeln. Der Verwaltungsapparat des Gerichts einschließlich seiner Spitze ist auf diese Weise für beide Instanzen nutzbar. Dementsprechend sind als Spruchkörper zwei Kammern vorgesehen: Die kleine Datenschutzkammer, besetzt mit dem Stellvertreter des Präsidenten als Vorsitzenden und zwei weiteren Richtern, bildet die erste Instanz; die große Datenschutzkammer, besetzt mit dem Präsidenten und vier weiteren Richtern, bildet die Beschwerdeinstanz.

Und noch eine Überlegung ergibt sich aus der Schaffung eines zentralen Gerichts für alle deutschen Diözesen und Ordensgemeinschaften: Auch, wenn Köln bzw. Bonn nicht weit von der Mitte Deutschlands entfernt liegt, würde die Reise dorthin einschließlich der Rückkehr eine erhebliche Zeit in Anspruch nehmen. Wäre nun in jedem Verfahren eine mündliche Verhandlung notwendig, so müsste jeder Betroffene (und jeder Richter) diese Reisezeit aufbringen, wollte er nicht Gefahr laufen, Verfahrensnachteile zu erleiden. In der Praxis wird es aber wohl regelmäßig um Rechtsfragen gehen, die sich auch ohne die leibliche Präsenz des Betroffenen bzw. seines Vertreters in angemessener Weise entscheiden lassen. Deswegen sieht das Verfahren eine freigestellte mündliche Verhandlung vor, was bedeutet, dass der Vorsitzende eine Verhandlung immer dann ansetzt, wenn er die Verletzung des rechtlichen Gehörs des Betroffenen befürchtet.

Richter des Datenschutzgerichts werden im Hinblick auf die wohl eher niedrigen Eingangszahlen zumindest in den ersten Jahren ihrer Tätigkeit mit Sicherheit nebenamtliche sein. Sie dürfen keine berufliche Verbindung zur Kirche haben, sollen kirchliche bzw. weltliche Juristen sein und Erfahrung in Datenschutzfragen besitzen. Natürlich gibt es Regelungen über den Ausschluss bzw. die Befangenheit eines Richters.

Das Verfahren

Es wird normalerweise durch die Einreichung einer Antragsschrift eingeleitet, in welcher der Antragsteller auch vorbringen muss, in eigenen Rechten betroffen zu sein. Sie kann wahlweise beim Gericht oder bei der Datenschutzaufsicht entweder binnen eines Jahres nach einem für den Betroffenen negativen Bescheid oder binnen drei Monaten der Untätigkeit eingereicht werden. Die Fristen bilden kein Zulässigkeitskriterium; vielmehr wird die Rechtsbehelfsberechtigung bei nutzlosem Verstreichen der Frist verwirkt. Typischerweise richtet sich das Verfahren gegen die Datenschutzaufsicht, doch kann auch direkt der Verantwortliche einer Dienststelle Antragsteller oder -gegner sein.

Nach Eingang der Antragsschrift hört das Gericht die Gegenseite an und bestimmt in den geschilderten Ausnahmefällen einen Termin zur mündlichen Verhandlung. Anlass für eine mündliche Verhandlung kann es aber auch sein, dass das Gericht Beweise erheben will. Es besteht der Amtsermittlungsgrundsatz; Beweise sind die auch in anderen Verfahren üblichen.

Mit oder ohne mündliche Verhandlung entscheidet die kleine Kammer durch Beschluss. Sie kann den Antrag als unzulässig verwerfen, ihn zurückweisen oder ihm stattgeben.

Gegen diesen Beschluss hat die unterlegene Partei die Möglichkeit der Beschwerde binnen einer (Verwirkungs-) Frist von drei Monaten. Das Verfahren in der zweiten Instanz entspricht demjenigen der ersten mit der Maßgabe, dass eine mündliche Verhandlung nur ganz ausnahmsweise stattfindet. Das Verfahren vor dem Datenschutzgericht endet mit der Mitteilung des Beschlusses der großen Kammer; eine dritte Instanz ist nicht vorgesehen.

Die Auswirkungen

Eine Entscheidung des Datenschutzgerichts wirkt sich auf die rechtlichen Verhältnisse der Beteiligten wie folgt aus:

- Hat das Datenschutzgericht festgestellt, dass eine Datenschutzverletzung vorlag, darf die kirchliche Dienststelle im staatlichen Zivilgerichtsverfahren über den Schadensersatz nicht vortragen, eine Datenschutzverletzung habe es nicht gegeben. Entsprechend ist für die positive Feststellung einer Datenschutzverletzung entweder eine Entscheidung der Datenschutzaufsicht oder des Datenschutzgerichts erforderlich. Damit ist eine Bindung über den Grund des Schadensersatzes deswegen hergestellt, weil es durch Art. 140 GG und Art. 137 WRV den staatlichen Gerichten verwehrt ist, über das Vorliegen einer Datenschutzverletzung zu entscheiden.
- Die Aufsichtsbehörde darf gegen einen Verantwortlichen keine Geldbuße verhängen, wenn das Datenschutzgericht festgestellt hat, eine Datenschutzverletzung habe nicht vorgelegen.