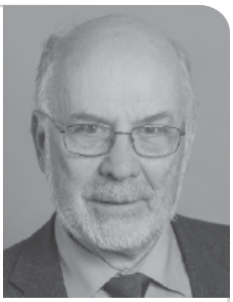
Jupp Joachimski

Jupp Joachimski ist seit seiner Pensionierung als Vorsitzender Richter am Bayerischen Obersten Landesgericht für die bayerischen (Erz-) Diözesen als Datenschutzbeauftragter tätig. 2015 hat er auch das Amt des Gemeinsamen Ordensdatenschutzbeauftragten der DOK Süd übernommen. Er hat zahlreiche Fachbücher zu Rechtsfragen veröffentlicht.



Jupp Joachimski

Das Datenschutzrecht der Ordensgemeinschaften

Der Datenschutz war in den Ordensgemeinschaften lange Zeit eher ein Stiefkind. Dies hatte mehrere Gründe: Zum einen war die technische Ausstattung der Orden bisher nicht wirklich so entwickelt, dass man ohne näheren Anlass über den Datenschutz viel hätte nachdenken müssen. Es erschien sogar vermessen, Grundsätze, die für Behörden oder Wirtschaftsunternehmen entwickelt worden waren, auf die Orden zu übertragen. Zum anderen haben sich die Ordensgemeinschaften auch deshalb nur wenig Gedanken darüber gemacht, wie der Datenschutz rechtlich zu organisieren ist, weil sie sich stark vom Gebot des Anstands im Rechtsverkehr leiten ließen und die Rücksichtnahme auf andere für sie eine Selbstverständlichkeit war. Aus Sorge um die Zukunft der Selbstverwaltungshoheit in Datenschutzbelangen hat die DOK die Initiative ergriffen und das Projekt „Gemeinsamer Ordensdatenschutzbeauftragter“ begonnen.

Die Prinzipien des Datenschutzrechts

Gegenstand

Grundsätzlich sind nur personenbezogene Daten Gegenstand des Datenschutzrechts. Eine Legaldefinition dafür gibt es in § 2 Abs. 1 Bundesdatenschutzgesetz, BDSG (entspricht § 2 Abs. 1 der Kirchlichen Datenschutzordnung, KDO): *Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).*

Das bedeutet: Einzelangaben über persönliche oder sachliche Verhältnisse sind alle Nennungen von 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.

Bestimmte Personen sind solche, die aufgrund der bezeichneten Angaben klar definiert sind. Bestimmbare 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!

Die Form der Daten
ist für den Datenschutz prinzipiell gleichgültig. Die Datenschutzregeln sind gleichermaßen anwendbar auf die Speicherung in Papierform oder in EDV-Form. Es gibt lediglich eine Sonderregelung für die Meldepflicht in § 3a KDO: Dort sind Verfahren automatisierter Verarbeitung von Daten angesprochen; darunter versteht man jede Art von elektronischer Datenverarbeitung unter Einsatz von Datenverarbeitungsanlagen (vgl. dazu § 2 Abs. 2 KDO). Darunter fallen auch einfache Textverarbeitungsprogramme und sogar Smartphones.

Was ist mit Bildern oder Filmen?
Abbildungen von *Personen* fallen nicht unter das Datenschutzrecht, weil sie in sich keine allgemein verständliche Aussage über die Person tragen. 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 11f. besprochen.
Die Videoüberwachung (§ 5 a KDO) ist des Zusammenhangs wegen auch in der kirchlichen Datenschutzordnung (bzw. dem BDSG) geregelt, obwohl bei der Videoüberwachung nur mittelbar personenbezogene Daten betroffen sind.

Grundprinzipien

Grundprinzipien des Datenschutzes sind:
- Datensicherheit
- Schutz gegen unbefugte Kenntnisnahme
- Auskunftspflicht.

Sie sind in allen Datenschutznormen geregelt und stellen sozusagen das „Skelett" des Datenschutzes dar.

Welche rechtlichen Vorschriften sind anzuwenden?

Das Datenschutzrecht ist deswegen besonders kompliziert, weil es in verschiedenen rechtlichen Ebenen Regelungen dazu gibt. Die Europäische Union hat 1995 eine Richtlinie zum Datenschutzrecht erlassen, welche nicht unmittelbares Recht wurde, sondern lediglich die Mitgliedstaaten bindet. Diese sind verpflichtet, ein nationales Datenschutzrecht zu erlassen, das die Mindeststandards der europäischen Richtlinie einhält.

Gegenwärtig verabschiedet die Europäische Union eine Datenschutz-Grundverordnung, welche im Gegensatz zur Richtlinie unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union werden soll. Mit dem Inkrafttreten dieser Grundverordnung ist Mitte des Jahres 2018 zu rechnen; bis dahin wird es sicher noch viele Anpassungen der KDO geben müssen. Sie bereiten derzeit allen kirchlichen Datenschutzbeauftragten viel Kopfzerbrechen.

Die Bundesrepublik Deutschland hat erstmals 1983 eine Datenschutzregelung erlassen, das Bundesdatenschutzgesetz (BDSG). Im kirchlichen Bereich ist es nicht anzuwenden, weil die Sonderregelung der kirchlichen Datenschutzordnung vorgeht. Allerdings wird bis zu einer entsprechenden Änderung der KDO § 42 a Bundesdatenschutzgesetz angewendet, gilt jedoch nur für kirchliche Krankenhäuser und Altenheime. Das Bundesdatenschutzgesetz ist allgemein anwendbar für

- Bundesbehörden
- Gerichte des Bundes und der Länder
- die Privatwirtschaft.

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 haben auch noch jeweils eigene Datenschutzvorschriften erlassen. Diese Landesdatenschutzgesetze gelten ausschließlich für die jeweiligen Landesbehörden. Neben diesen Datenschutzgesetzen gibt es noch besondere Regelungen in den einzelnen Bundesländern für bestimmte Fachgebiete. Am wichtigsten sind die Regelungen für das Schulwesen (Beispiel: §§ 120ff. Schulgesetz NRW) und die Krankenhäuser (Beispiel: Art. 27 des bayerischen Gesetzes über das Krankenhauswesen).

In Art. 137ff. der Weimarer Reichsverfassung wurde den „Religionsgesellschaften“ das Recht der Selbstverwaltung vorbehalten. Dieses Recht hat das Grundgesetz in Art. 140 für die Bundesrepublik Deutschland fortgeschrieben. Soweit also die Selbstverwaltungshoheit des Grundgesetzes reicht, dürfen insbesondere die Kirchen, also insbesondere die evangelische und katholische, ihre inneren Angelegenheiten selbst verwalten.

In Ausübung dieses Selbstverwaltungsrechts haben 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 an öffentlich-rechtliche Religionsgesellschaften nur dann zulässig ist, wenn bei ihnen ausreichende Vorkehrungen für den Datenschutz getroffen sind. Das bedeutet: Der Bundesgesetzgeber geht 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.

In der katholischen Kirche ist es die KDO (= Anordnung über den kirchlichen Datenschutz, Quelle: Webseite des jeweiligen Bistums oder www.datenschutz-kirche.de). Die evangelische Kirche hat ein Datenschutzgesetz vom 1.1.2013. Nach Art. 85 des Entwurfes der neuen EU-Datenschutzverordnung bleiben diese Regelungen auch nach Inkrafttreten

der Verordnung gültig, sofern sie den Standards der Verordnung entsprechen.

Die wichtigsten Regelungen der Kirchlichen Datenschutzordnung

Die KDO gilt in der gesamten verfassten Kirche kraft bischöflicher Anordnungen, die auch für die Orden bischöflichen Rechts wirken. Erfasst sind alle kirchlichen Einrichtungen ohne Rücksicht auf ihre Rechtsform. In den Ordensgemeinschaften päpstlichen Rechts muss die KDO durch besonderen Rechtsetzungsakt des Ordensoberen in Kraft gesetzt werden.
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 Ordensgemeinschaften 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; diese werden von der KDO nicht berührt.
Für normale kirchliche Dienststellen ist § 1 Abs. 2 eindeutig; sie unterfallen immer der KDO. Kritisch wird es jedoch nach § 1 Abs. 2 Nummer 3, soweit sich die Kirche privatrechtlicher Organisationsformen bedient. Zu diesen zählen diejenigen des bürgerlichen Rechts (Vereine) oder des Handelsrechts (Aktiengesellschaft, Gesellschaft mit beschränkter Haftung, Genossenschaft u. ä.). Die KDO gilt für derartige Organisationsformen nur dann, wenn die so genannte „Kirchlichkeitsprüfung“ erfüllt wird. Eine solche Organisation ist nur dann eine kirchliche Dienststelle im Sinne der KDO, 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 sind eine Mineralwasser-Vertriebsgesellschaft oder ein Golfplatz nicht ohne weiteres kirchliche Dienststellen, auch wenn sie von der Kirche oder einer Ordensgemeinschaft betrieben wird. Ein besonderer Streitfall ist häufig die Kirchenzeitung. Bei ihnen wird zu prüfen sein, ob die Gewinnerzielung im Vordergrund steht oder die Kommunikation mit den Mitgliedern der Kirche, wohl der Regelfall.

Geltung anderer Rechtsnormen
Nach ihrem eigenen Verständnis ist die kirchliche Datenschutzordnung gegenüber spezielleren Vorschriften subsidiär, d.h. nicht die KDO, sondern diese Vorschriften sind anzuwenden (§1 Abs.3 KDO). Das gilt insbesondere im Verhältnis zu den Vorschriften der kirchlichen Archivordnung, und landesgesetzlichen Vorschriften über den Datenschutz in Krankenhäusern und Schulen.

Die Rechtmäßigkeit des Umgangs mit den Daten
Ausgangspunkt dafür ist § 3 KDO: Der Umgang mit personenbezogenen Daten ist nur zulässig, soweit die KDO oder eine staatliche Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Diese Vorschrift ist die zentrale Handlungsanweisung der KDO. Die KDO erlaubt einen Umgang mit Daten auf jeden Fall immer dann, wenn

zur Erfüllung der Aufgaben der Dienststelle nötig ist. Es muss daher immer zuerst geprüft werden, ob die kirchliche Dienststelle eine entsprechende Aufgabe zum Umgang mit diesen speziellen Daten hat. Die allgemeine Prüfungsreihenfolge für den Umgang einer kirchlichen Dienststelle mit Daten ist daher:

- Liegt eine entsprechende Aufgabe (objektiv) vor?
- Besteht sonst ein Rechtfertigungsgrund nach § 10 Abs. 2 KDO für den Umgang mit den Daten, insbesondere: Hat der Betroffene eingewilligt?

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 § 10a KDO, vgl. dazu die Ausführungen weiter unten.

Die Begriffsbestimmungen des § 2 KDO entsprechen der Regelung im Bundesdatenschutzgesetz. Die Vorschrift sollte immer herangezogen werden, wenn die Bedeutung eines Begriffes unklar ist. Aus den zahlreichen Begriffsbestimmungen sollen zwei herausgehoben werden:

- Die besonderen Arten der personenbezogenen Daten (§ 2 Nr. 10 KDO) 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 § 2 Nr. 12 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 §4 Satz 2 KDO verpflichtet werden müssen.

Datenerhebung

Der Begriff wird in § 2 Abs. 3 definiert als das „Beschaffen von Daten über den Betroffenen". 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 § 15 Abs.4 BDSG 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 § 6 KDO so sichern, dass

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

§ 6 KDO lautet: *Kirchliche Stellen im Geltungsbereich des § 1 Abs. 2, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Anordnung, insbesondere die in der Anlage zu dieser Anordnung genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.*
Eigentlich müsste die KDO tausende oder gar Millionen von Situationen schildern und jeweils darlegen, welche Sicherheitsmaßnahmen für die Daten erforderlich sind; das tut sie aber 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-Mailverkehr 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 kirchliche Dienststellen nicht so interessant für Hacker sind wie zum Beispiel das Verteidigungsministerium oder die NASA. Deswegen kann im normalen Verfahren das E-Mail benutzt werden, nicht jedoch dann, wenn besondere Arten personenbezogener Daten im Sinne des § 2 Nr. 10 KDO darin enthalten sind. Bei DE-Mail bestehen jedenfalls ähnliche Einschränkungen, solange eine Zwischenverarbeitung stattfindet. Eine Möglichkeit wäre die Verschlüsselung der E-Mails, die sogar mit Freeware-Programmen (z.B. Boxcryptor) möglich ist.
- 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 Pfarrsekretärin-

nen 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 außerhalb von EU und Europäischem Wirtschaftsraum (EWR), 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 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. Für die Verwendung zu privaten Zwecken gibt es auf der allen Ordensgemeinschaften mitgeteilten Downloadseite Tipps zur datenschutzgerechten Einstellung.

Beim Lesen ist vielleicht schon zu erkennen, dass dies alles 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 KDO 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 ist bei kleineren Dienststellen wie Kirchenstiftungen schon das sog. „Erweiterte Verfahrensverzeichnis". Man sollte dieses Muster aber nicht nur ausfüllen, sondern die Gelegenheit nutzen, eine Bestandsaufnahme zu fertigen.

Verpflichtungserklärung

Zu den organisatorischen Maßnahmen im Sinne des § 6 KDO gehört es auch, dass die mit den Daten befassten Personen sich zum Schutz des Datengeheim-

nisses verpflichtet haben. Diese Verpflichtung ist in § 4 Satz 2 KDO 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 § 4 KDO nur dann zulässig, wenn eine Rechtfertigung gemäß § 10 KDO vorliegt. In dieser Vorschrift bildet wiederum Abs. 1 Satz 1 die zentrale Norm. Es ist also in jedem Fall zu prüfen, ob der beabsichtigte Umgang mit den Daten – Erheben, Speichern oder Verändern – 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:

- In die Ministrantenliste eines Pfarrbüros soll der Familienstand der Eltern der jeweiligen Ministranten aufgenommen werden. Für diese bloße Datenspeicherung 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.
- 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 KDO. Dafür gibt es keine entsprechende Aufgabe der Kirchenstiftung.
- 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 § 1 Abs. 2 Nr. 2 KDO. Eine Datenübermittlung an sie richtet sich daher nach § 11 KDO. Gemäß § 11 Abs. 2 Satz 2 KDO 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

Weitergabe von Daten
Werden die Daten von der Dienststelle weitergegeben, so müssen zusätzlich zur Prüfung der Aufgabe im Sinne des § 10 KDO die §§ 11 und 12 KDO bemüht werden. Zu prüfen ist also: Gehen die Daten...

- ...an eine kirchliche oder staatliche Stelle (§ 11 KDO) - § 11 Abs. 1: Wiederum ist die Aufgabe der Ausgangs- oder Empfangsstelle entscheidend.

oder

- ...an einen Dritten bzw. an die ganze Welt (Fall der Veröffentlichung) § 12. Entscheidend ist die Aufgabe der Ausgangsstelle oder das berechtigte Interesse des Dritten.

Besonders zu beachten ist im Falle des § 11 dessen Abs.2 S.2-4: Erfolgt die Übermittlung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen 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 notwendigerweise selbst 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 § 11 Abs.4 KDO 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.

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 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 (§ 3 Abs.2 KDO). Die Einwilligung muss auf Freiwilligkeit beruhen (§ 3 Abs. 2 Satz 2 KDO). 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 Sonderform der Übermittlung: Datenverarbeitung im Auftrag, § 8 KDO

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 solchen Vorgängen ist die Einhaltung von § 8 Abs. 2 KDO. 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.

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 (§ 14 Abs. 2 KDO). 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 wiederhergestellt 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.
Nicht gelöscht werden dürfen Daten, für die es gesetzliche Aufbewahrungsfristen gibt, § 14 Abs. 3 Nummer 1 KDO.

Eine Zusammenstellung gesetzlicher Aufbewahrungsfristen von Sozialdaten finden Sie im Internet unter www.datenschutzkirche.de.

Auskunft

Das Gegenstück zum Recht der Dienststelle auf Speicherung der Daten von Betroffenen ist deren Auskunftsrecht nach § 13 KDO. 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.

Besonderheiten des Mitarbeiterdatenschutzes

Der Mitarbeiterdatenschutz ist sowohl im Bundesdatenschutzgesetz wie auch in der Kirchlichen Datenschutzordnung eher stiefmütterlich behandelt. Das liegt daran, dass schon vor Inkrafttreten des Bundesdatenschutzgesetzes die Rechtsstellung des Bundesarbeitsgerichtes den Arbeitnehmern bestimmte Datenschutzrechte sicherte. Als es dann in das BDSG § 32 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. § 10 a KDO entspricht im Wortlaut fast vollständig dem § 32 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.
- 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 sein 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.

Exkurs 1: Videoüberwachung

Wie schon oben dargestellt, wird die Videoüberwachung in der KDO aus Gründen des Zusammenhangs in § 5a KDO 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. Die KDO 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 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. Auf die Tatsache der Videoüberwachung muss durch geeignete Maßnahmen – in der Regel durch ein Hinweisschild – hingewiesen werden, § 5a Abs. 2 KDO.
- 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

Ausgangspunkt ist § 22 Kunsturhebergesetz: Bilder dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.
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 Konsequenz aus dieser Vorschrift ist, dass die Veröffentlichung ohne 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.
Von dieser Vorschrift des § 22 gibt es Ausnahmen. Für den kirchlichen Bereich am bedeutsamsten ist die Ausnahme in Absatz 1 Nummer 3: Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben, dürfen ohne Einverständnis des Abgebildeten veröffentlicht werden.
Die hier verwendeten Begriffe „Versammlung“ und „Aufzug“ sind sehr weit auszulegen. Hierunter werden alle Ansammlungen von Menschen, die den kollektiven Willen haben, etwas gemeinsam zu tun, verstanden. 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.
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.

Die Datenschutzbeauftragten

Der Diözesan- oder Ordensdatenschutzbeauftragte, § 16 KDO
Sie stehen einander 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 Ordensdatenschutzbeauftragten gemünzt; sie gelten in gleicher Weise für den Diözesandatenschutzbeauftragten. Abweichungen hebe ich hervor.

Autoreninfo

Die genauen Angaben zum Autor finden Sie in der gedruckten Ausgabe.

Der Ordensdatenschutzbeauftragte ist die höchste vom Ordensoberen berufene Datenschutzinstanz. Die KDO sieht ausdrücklich vor, dass ein Ordensdatenschutzbeauftragter für mehrere Orden bestellt werden kann (§ 16 Abs. 2 Satz 5 KDO). Der Ordensdatenschutzbeauftragte 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 Ordensdatenschutzbeauftragten erfolgt für mindestens vier und höchstens acht Jahre. Eine vorzeitige Abberufung ist nur unter engen Voraussetzungen möglich; allerdings kann der Ordensdatenschutzbeauftragte sein

Amt vorzeitig zurückgeben. Im Verhältnis zu den Ordensgemeinschaften hat er ein Weisungsrecht (vgl. § 17 Abs. 2 KDO). Er berät sie 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 Ordensdatenschutzbeauftragte über die Einhaltung der kirchlichen Datenschutzordnung sowie der anderen kirchlichen und staatlichen Vorschriften über den Datenschutz in seinem Bereich. Jedermann kann ihn gemäß § 15 KDO anrufen, wenn er sich in seinen Datenschutzrechten verletzt fühlt. Insofern hat der Ordensdatenschutzbeauftragte eine gerichtsähnliche Funktion (vgl. auch § 17 Abs. 1 KDO). Stellt er nach Prüfung des Sachverhalts (§ 15 Abs. 2 KDO) 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 (§19 Abs. 1 KDO).

Die Dienststellen der Ordensgemeinschaft sind nach § 3a Abs. 1 KDO verpflichtet, Verfahren automatisierter Verarbeitung vor Inbetriebnahme dem Ordensdatenschutzbeauftragten zu melden. Diese Vorschrift dürfte diejenige in der kirchlichen Datenschutzordnung sein, gegen die am meisten zuwidergehandelt wird. Die Meldepflicht entfällt allerdings, wenn für die Dienststelle ein betrieblicher Datenschutzbeauftragter nach § 20 KDO bestellt wurde. Muster für Meldungen finden sich in der erwähnten Downloadseite.

Der Ordensdatenschutzbeauftragte 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 § 17 Abs. 3 und 4 eine angemessene Personalausstattung zu. Das Personal wird zwar von der DOK beauftragt, doch untersteht es der ausschließlichen Weisungsbefugnis des Ordensdatenschutzbeauftragten.

Der betriebliche Datenschutzbeauftragte, § 20 KDO

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 Ordensdatenschutzbeauftragten fast unmöglich. 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 § 20 Abs. 1 KDO 2014 „sollen“ betriebliche Beauftragte für den Datenschutz bestellt werden. Dieses „Sollen“ wandelt sich auf Grund bereichsspezifischer Regelungen, z. B. im Krankenhausdatenschutzbereich, zu einem „Müssen“. Kirchliche bzw. staatliche Gesetze, soweit diese für den kirchlichen Bereich zur Anwendung kommen, schreiben

gelegentlich die Berufung eines betrieblichen Beauftragten für den Datenschutz vor. In anderen Fällen verdichtet sich das „Können“ zu einer „Notwendigkeit“, wenn auf Grund der Größe der Dienststelle oder der Einrichtung, oder wenn auf Grund der verarbeiteten Datenmenge eine erhöhte Schutzwürdigkeit eine unabhängige Vorortkontrolle und Vorortüberwachung aufdrängt.
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.
Außerdem gibt es rechtlichen Druck für die Bestellung eines betrieblichen Datenschutzbeauftragten: Die Nichtbestellung hat unter Umständen zur Folge, dass eine Meldepflicht nach § 3a KDO entsteht. § 3a Abs.1 KDO 2014 schreibt eine Meldepflicht (des Dienststellenleiters) an den Diözesandatenschutzbeauftragten in Bezug auf jede automatisierte Verarbeitung vor deren Inbetriebnahme vor. Nur wenn ein betrieblicher Datenschutzbeauftragter bestellt ist, kann auf die Verfahrensmeldungen verzichtet werden.

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! Der Dienststellenleiter – bei Ordensgemeinschaften der Ordensobere – bestellt den betrieblichen Datenschutzbeauftragten durch schriftliche Anordnung.

Rechtsstellung
Der 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 die KDO, dass er in der Ausübung seiner Fachkunde weisungsfrei ist. 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.
Ganz generell ist überhaupt der betriebliche Auge und Ohr des Ordensdatenschutzbeauftragten. Dieser wendet sich zum Beispiel bei Beschwerden über eine Einrichtung immer erst an den betrieblichen, bittet ihn um Sachverhaltsaufklärung und hört ihn an. Umgekehrt versorgt der Ordensdatenschutzbeauftragte den betrieblichen mit den notwendigen Informationen und ist immer für ihn zu sprechen.