Datenschutz und Melderecht der katholischen Kirche

4., korrigierte und ergänzte Auflage 2017

1. Dezember 2006

Datenschutz und Melderecht der katholischen Kirche / hrsg. vom Sekretariat der Deutschen Bischofskonferenz. – 4., korrigierte und ergänzte Aufl. – Bonn 2017. – 154 S. – (Arbeitshilfen ; 206)

INHALT

1. Vorwort

Der Verband der Diözesen Deutschlands hat durch Beschlüsse seiner Vollversammlung am 23.06.2003, 25.11.2003 und am 20./21.06.2005 die nachstehend abgedruckten Muster

- einer „Anordnung über den kirchlichen Datenschutz (KDO)“,
- einer „Durchführungsverordnung zur KDO“,
- einer „Anordnung zum Sozialdatenschutz der freien Jugendhilfe“ sowie
- einer „Kirchlichen Meldewesenanordnung (KMAO)“

verabschiedet und den Diözesen die Umsetzung in diözesanes Recht empfohlen.

Dies ist zwischenzeitlich geschehen. Die genauen Fundstellen in den diözesanen Amtsblättern ergeben sich aus der auf Seite 123 f. abgedruckten Übersicht. Diese wurde im Verhältnis zur Vorauflage erweitert und enthält jetzt auch Fundstellen datenschutzrechtlicher Spezialregelungen für Krankenhäuser, Schulen etc.

Um das Verständnis sowohl der „Anordnung über den kirchlichen Datenschutz“ als auch der „Kirchlichen Meldewesenanordnung“ zu erleichtern, enthält die Broschüre eine in der Kommission für Meldewesen und Datenschutz des Verbandes der Diözesen Deutschlands abgestimmte erste Einführung in die nicht immer ganz leichten Rechtsmaterien. Sie will weder einen Kommentar, noch den Austausch mit dem Diözesandatenschutzbeauftragten ersetzen, der in Zweifelsfällen immer zu Rate gezogen werden sollte.

Bonn, 01. Dezember 2006

P. Dr. Hans Langendörfer SJ
Sekretär der Deutschen Bischofskonferenz

2. Anordnung über den kirchlichen Datenschutz (KDO)

Präambel

Aufgabe der Datenverarbeitung im kirchlichen Bereich ist es, die Tätigkeit der Dienststellen und Einrichtungen der Katholischen Kirche zu fördern. Dabei muss gewährleistet sein, dass der Einzelne durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht geschützt wird. Aufgrund des Rechtes der Katholischen Kirche, ihre Angelegenheiten selbst zu regeln, wird zu diesem Zweck die folgende Anordnung erlassen:

§ 1
Zweck und Anwendungsbereich

(1) Zweck dieser Anordnung ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Diese Anordnung gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch:

1. das Bistum, die Kirchengemeinden, die Kirchenstiftungen und die Kirchengemeindeverbände,
2. den Deutschen Caritasverband, die Diözesan-Caritasverbände, ihre Untergliederungen und ihre Fachverbände ohne Rücksicht auf ihre Rechtsform,
3. die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform.

(3) Soweit besondere kirchliche oder staatliche Rechtsvorschriften auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieser Anordnung vor. Die Verpflichtung zur Wahrung des Beicht- und Seelsorgegeheimnisses, anderer gesetzlicher Geheimhaltungspflichten oder von anderen Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 2
Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren,

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

   a) die Daten an den Dritten weitergegeben werden oder

   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(7) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(8) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(9) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie

diejenigen Personen und Stellen, die im Geltungsbereich dieser Anordnung personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(10) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Dazu gehört nicht die Zugehörigkeit zu einer Kirche oder sonstigen Religionsgemeinschaft.

(11) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,
2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

(12) Beschäftigte sind insbesondere

1. Kleriker, Kandidaten für das Priesteramt oder in einem kirchlichen Beamtenverhältnis stehende Personen,
2. Ordensangehörige, soweit sie auf einer Planstelle in einer Einrichtung der eigenen Ordensgemeinschaft oder aufgrund eines Gestellungsvertrages tätig sind,
3. in einem Arbeitsverhältnis stehende Personen,
4. zu ihrer Berufsbildung tätige Personen mit Ausnahme der Postulanten und Novizen,
5. Teilnehmende an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobungen (Rehabilitationen),

6. in anerkannten Werkstätten für behinderte Menschen tätige Personen,
7. nach dem Bundesfreiwilligendienstgesetz oder in vergleichbaren Diensten tätige Personen,
8. Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
9. sich für ein Beschäftigungsverhältnis Bewerbende sowie Personen, deren Beschäftigungsverhältnis beendet ist.

§ 2a
Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und der Aufwand nicht außer Verhältnis zum angestrebten Schutzzweck steht.

§ 3
Zulässigkeit der Datenerhebung, -verarbeitung oder -nutzung

(1) Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, soweit

1. diese Anordnung oder eine andere kirchliche oder eine staatliche Rechtsvorschrift sie erlaubt oder anordnet oder
2. der Betroffene eingewilligt hat.

(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Sie bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

(3) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Abs. 2 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Abs. 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.

(4) Soweit besondere Arten personenbezogener Daten (§ 2 Abs. 10) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 2 Abs. 10) verarbeitet werden oder

2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(6) Zuständig für die Vorabkontrolle ist der betriebliche Datenschutzbeauftragte; soweit kein betrieblicher Datenschutzbeauftragter bestellt ist, ist für die Vorabkontrolle der Diözesandatenschutzbeauftragte zuständig.

§ 3a
Meldepflicht und Verzeichnis

(1) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, Verfahren automatisierter Verarbeitung vor Inbetriebnahme dem Diözesandatenschutzbeauftragten zu melden.

(2) Die Meldung hat folgende Angaben zu enthalten

1. Name und Anschrift der verantwortlichen Stelle,
2. Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung der Stelle berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
4. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

5. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
6. Regelfristen für die Löschung der Daten,
7. eine geplante Datenübermittlung ins Ausland,
8. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 6 KDO zur Gewährleistung der Sicherheit der Bearbeitung angemessen sind,
9. zugriffsberechtigte Personen.

(3) Die Meldepflicht entfällt, wenn für die verantwortliche Stelle ein betrieblicher Datenschutzbeauftragter nach § 20 bestellt wurde. Sie entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens zehn Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) Die Angaben nach Abs. 2 sind von der kirchlichen Stelle in einem Verzeichnis vorzuhalten. Sie macht die Angaben nach Abs. 2 Nr. 1 bis 7 auf Antrag jedermann in geeigneter Weise verfügbar, der ein berechtigtes Interesse nachweist.

§ 4
Datengeheimnis

Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten

oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 5
Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§ 13) und auf Berichtigung, Löschung oder Sperrung (§ 14) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in einer Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene zu unterrichten.

§ 5a
Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung
   oder zur Wahrnehmung des Hausrechts oder
2. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend § 13a zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 5b
Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,

3. darüber, wie er seine Rechte nach den §§ 13 und 14 ausüben kann und über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 6
Technische und organisatorische Maßnahmen

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.

§ 7
Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Be-

rücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufes bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 6 erforderliche technische und organisatorische Maßnahmen.

(3) Über die Einrichtung von Abrufverfahren ist der Diözesandatenschutzbeauftragte unter Mitteilung der Festlegungen des Abs. 2 zu unterrichten.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts nutzen kann.

§ 8
Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieser Anordnung und anderer Vorschriften über den Datenschutz verantwortlich. Die in § 5 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 6 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum

Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen diese Anordnung oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Die Absätze 1 bis 3 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 9
Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stellen erforderlich ist.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden sie beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen ist er über die Rechtsvor-

schrift und über die Folgen der Verweigerung von Angaben aufzuklären.

(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nichtkirchlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft ermächtigt, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(5) Das Erheben besonderer Arten personenbezogener Daten (§ 2 Abs. 10) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder dies aus Gründen eines wichtigen öffentlichen Interesses zwingend erforderlich ist,
2. der Betroffene nach Maßgabe des § 3 Abs. 4 eingewilligt hat,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat oder es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich ist,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist oder dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
6. der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert,
7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder

Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,

8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,
9. dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist.

§ 10
Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt und kirchliche Interessen nicht entgegenstehen,
2. der Betroffene eingewilligt hat,

3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr einer Gefahr für die öffentliche Sicherheit oder erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung

auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

10. der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 2 Abs. 10) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 9 Abs. 5 Nr. 1 bis 6 oder 9 zulassen würden oder
2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das kirchliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des kirchlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 2 Abs. 10) zu den in § 9 Abs. 5 Nr. 7 genannten Zwecken richtet sich nach den für die in § 9 Abs. 5 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 10a
Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten einschließlich der Daten über die Religionszugehörigkeit, die religiöse Überzeugung und die Erfüllung von Loyalitätsobliegenheiten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind oder eine Rechtsvorschrift dies vorsieht.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte nach der jeweils geltenden Mitarbeitervertretungsordnung bleiben unberührt.

§ 11
Datenübermittlung an kirchliche und öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an Stellen im Geltungsbereich des § 1 ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. 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. § 7 Abs. 4 bleibt unberührt.

(3) Die empfangende kirchliche Stelle darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 10 Abs. 2 zulässig

(4) Für die Übermittlung personenbezogener Daten an öffentliche Stellen und an kirchliche Stellen außerhalb des Geltungsbereichs des § 1 gelten die Abs. 1–3 entsprechend, sofern sichergestellt ist, dass bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Abs. 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Abs. 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer kirchlichen Stelle weitergegeben werden.

§ 12
Datenübermittlung an nicht kirchliche und nicht öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht kirchliche Stellen, nicht öffentliche Stellen oder Personen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden, oder
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten

personenbezogener Daten (§ 2 Abs. 10) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 10 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, wenn die Unterrichtung wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen nicht geboten erscheint, wenn die Unterrichtung die öffentliche Sicherheit gefährden oder dem kirchlichen Wohl Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 13
Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über:

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Das Bistum bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung.

(2) Abs. 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsgemäßer oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft dem kirchlichen Wohl Nachteile bereiten würde,
3. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden würde,

4. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen oder rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Diözesandatenschutzbeauftragten wenden kann.

(5) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Diözesandatenschutzbeauftragten zu erteilen, soweit nicht das Bistum im Einzelfall feststellt, dass dadurch das kirchliche Wohl beeinträchtigt wird. Die Mitteilung des Diözesandatenschutzbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(6) Die Auskunft ist unentgeltlich.

§ 13a
Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit

der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
3. die Speicherung oder Übermittlung der personenbezogenen Daten durch eine Rechtsvorschrift ausdrücklich vorgesehen ist.

(3) § 13 Abs. 2 und 3 gelten entsprechend.

§ 14
Berichtigung, Löschung oder Sperrung von Daten; Widerspruchsrecht

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die verantwortliche Stelle im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen, im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

§ 15
Anrufung des Diözesandatenschutzbeauftragten

(1) Wer der Ansicht ist, dass bei der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Stellen gemäß § 1 Abs. 2 gegen Vorschriften dieser Anordnung oder gegen andere Datenschutzvorschriften verstoßen worden ist oder ein solcher Verstoß bevorsteht, kann sich unmittelbar an den Diözesandatenschutzbeauftragten wenden.

(2) Auf ein solches Vorbringen hin prüft der Diözesandatenschutzbeauftragte den Sachverhalt. Er fordert die betroffene kirchliche Dienststelle zur Stellungnahme auf, soweit der Inhalt des Vorbringens den Tatbestand einer Datenschutzverletzung erfüllt.

(3) Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an den Diözesandatenschutzbeauftragten gewendet hat.

§ 16
Bestellung des Diözesandatenschutzbeauftragten

(1) Der Bischof bestellt für den Bereich seines Bistums einen Diözesandatenschutzbeauftragten; die Bestellung erfolgt für die Dauer von mindestens vier, höchstens acht Jahren. Die mehrmalige erneute Bestellung ist zulässig. Die Bestellung als Datenschutzbeauftragter für mehrere Diözesen und/oder Ordensgemeinschaften ist zulässig.

(2) Zum Diözesandatenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Er soll die Befähigung zum Richteramt gemäß § 5 Deutsches Richtergesetz haben und muss der Katholischen Kirche angehören. Der Diözesandatenschutzbeauftragte ist auf die gewissenhafte Erfüllung seiner Pflichten und die Einhaltung des kirchlichen und des für die Kirchen verbindlichen staatlichen Rechts zu verpflichten. Anderweitige Tätigkeiten dürfen das Vertrauen in die Unabhängigkeit und Unparteilichkeit des Diözesandatenschutzbeauftragten nicht gefährden. Dem steht eine Bestellung als Diözesandatenschutzbeauftragter für mehrere Diözesen und/oder Ordensgemeinschaften nicht entgegen.

(3) Die Bestellung kann vor Ablauf der Amtszeit widerrufen werden, wenn Gründe nach § 24 Deutsches Richtergesetz vorliegen, die bei einem Richter auf Lebenszeit dessen Entlassung aus dem Dienst rechtfertigen, oder Gründe vorliegen, die nach der Grundordnung des kirchlichen Dienstes im Rahmen kirchlicher Arbeitsverhältnisse in der jeweils

geltenden Fassung eine Kündigung rechtfertigen. Auf Antrag des Beauftragten nimmt der Bischof die Bestellung zurück.

§ 17
Rechtsstellung des Diözesandatenschutzbeauftragten

(1) Der Diözesandatenschutzbeauftragte ist in Ausübung seiner Tätigkeit an Weisungen nicht gebunden und nur dem kirchlichen Recht und dem für die Kirchen verbindlichen staatlichen Recht unterworfen.
Die Ausübung seiner Tätigkeit geschieht in organisatorischer und sachlicher Unabhängigkeit. Die Dienstaufsicht ist so zu regeln, dass dadurch die Unabhängigkeit nicht beeinträchtigt wird.

(2) Das der Bestellung zum Diözesandatenschutzbeauftragten zugrunde liegende Dienstverhältnis kann während der Amtszeit nur unter den Voraussetzungen des § 16 Abs. 3 beendet werden. Dieser Kündigungsschutz wirkt für den Zeitraum von einem Jahr nach der Beendigung der Amtszeit entsprechend fort, soweit ein kirchliches Beschäftigungsverhältnis fortgeführt wird oder sich anschließt.

(3) Dem Diözesandatenschutzbeauftragten wird die für die Erfüllung seiner Aufgaben angemessene Personal- und Sachausstattung zur Verfügung gestellt. Er verfügt über einen eigenen jährlichen Haushalt, der gesondert auszuweisen ist und veröffentlicht wird.

(4) Der Diözesandatenschutzbeauftragte wählt das notwendige Personal aus, das von einer kirchlichen Stelle angestellt wird. Die vom Diözesandatenschutzbeauftragten ausgewählten und von dieser kirchlichen Stelle angestellten Mitarbeiter unterstehen der Dienst- und Fachaufsicht des Diözesandatenschutzbeauftragten und können nur mit seinem

Einverständnis von der kirchlichen Stelle gekündigt, versetzt oder abgeordnet werden.

(5) Der Diözesandatenschutzbeauftragte ist oberste Dienstbehörde im Sinne des § 96 Strafprozessordnung. Er trifft die Entscheidung über Aussagegenehmigungen für seinen Bereich in eigener Verantwortung. Der Diözesandatenschutzbeauftragte ist oberste Aufsichtsbehörde im Sinne des § 99 Verwaltungsgerichtsordnung.

(6) Der Diözesandatenschutzbeauftragte bestellt im Einvernehmen mit dem Diözesanbischof einen Vertreter, der im Fall seiner Verhinderung die unaufschiebbaren Entscheidungen trifft. Für den Vertreter gilt § 16 Abs. 2 entsprechend.

(7) Der Diözesandatenschutzbeauftragte ist, auch nach Beendigung seines Auftrages, verpflichtet, über die ihm in seiner Eigenschaft als Diözesandatenschutzbeauftragtem bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(8) Der Diözesandatenschutzbeauftragte darf, auch wenn sein Auftrag beendet ist, über solche Angelegenheiten ohne Genehmigung des Bischofs weder vor Gericht noch außergerichtlich Aussagen oder Erklärungen abgeben. Die Genehmigung, als Zeuge auszusagen, wird in der Regel erteilt. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen.

§ 18
Aufgaben des Diözesandatenschutzbeauftragten

(1) Der Diözesandatenschutzbeauftragte wacht über die Einhaltung der Vorschriften dieser Anordnung sowie anderer

Vorschriften über den Datenschutz. Er kann Empfehlungen zur Verbesserung des Datenschutzes geben. Des Weiteren kann er die bischöfliche Behörde und sonstige kirchliche Dienststellen in seinem Bereich in Fragen des Datenschutzes beraten. Auf Anforderung der bischöflichen Behörde hat der Diözesandatenschutzbeauftragte Gutachten zu erstellen und Berichte zu erstatten.

(2) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, den Diözesandatenschutzbeauftragten bei der Erfüllung seiner Aufgaben zur unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme,
2. während der Dienstzeit Zutritt zu allen Diensträumen, die der Verarbeitung und Aufbewahrung automatisierter Dateien dienen, zu gewähren,

soweit nicht sonstige kirchliche Vorschriften entgegenstehen.

(3) Der Diözesandatenschutzbeauftragte erstellt jährlich einen Tätigkeitsbericht, der dem Bischof vorgelegt und der Öffentlichkeit zugänglich gemacht wird. Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklungen des Datenschutzes im nichtkirchlichen Bereich enthalten.

(4) Der Diözesandatenschutzbeauftragte wirkt auf die Zusammenarbeit mit den kirchlichen Stellen, insbesondere mit den anderen Diözesandatenschutzbeauftragten, hin.

(5) Zu seinem Aufgabenbereich gehört die Zusammenarbeit mit den staatlichen Beauftragten für den Datenschutz.

§ 19
Beanstandungen durch den Diözesandatenschutzbeauftragten

(1) Stellt der Diözesandatenschutzbeauftragte Verstöße gegen Vorschriften dieser Anordnung oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er diese unter Setzung einer angemessenen Frist zur Behebung gegenüber der betroffenen kirchlichen Dienststelle.

(2) Wird die Beanstandung nicht fristgerecht behoben, so verständigt der Diözesandatenschutzbeauftragte die Aufsicht führende Stelle und fordert sie zu einer Stellungnahme auf.

(3) Der Diözesandatenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der Aufsicht führenden Stelle verzichten, wenn es sich um unerhebliche Mängel handelt, deren Behebung mittlerweile erfolgt ist.

(4) Mit der Beanstandung kann der Diözesandatenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(5) Die gemäß Abs. 2 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandungen des Diözesandatenschutzbeauftragten getroffen worden sind.

(6) Zur Gewährleistung der Vorschriften dieser Anordnung und anderer Vorschriften über den Datenschutz kann der Diözesandatenschutzbeauftragte gegenüber der betroffenen Dienststelle Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer und organisa-

torischer Mängel anordnen. Wird diese Anordnung nicht fristgemäß umgesetzt, hat sich der Diözesandatenschutzbeauftragte an die Aufsicht führende Stelle zu wenden, die zeitnah über die notwendigen Maßnahmen entscheidet.

§ 20
Betrieblicher Beauftragter für den Datenschutz

(1) Kirchliche Stellen im Sinne des § 1 Abs. 2, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, können einen betrieblichen Datenschutzbeauftragten schriftlich bestellen.

(2) Sind mit der automatisierten Datenerhebung, -verarbeitung oder -nutzung mehr als zehn Personen befasst, so soll ein betrieblicher Datenschutzbeauftragter bestellt werden.

(3) Zum betrieblichen Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der kirchlichen Stelle betraut werden. Ein betrieblicher Datenschutzbeauftragter kann von mehreren kirchlichen Stellen bestellt werden.

(4) Der betriebliche Datenschutzbeauftragte ist dem Leiter der kirchlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.

(5) Die kirchlichen Stellen haben den betrieblichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Betroffene können sich jederzeit an den betrieblichen Datenschutzbeauftragten wenden.

(6) Ist ein betrieblicher Beauftragter für den Datenschutz bestellt worden, so ist die Kündigung seines Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung der Kündigungsfrist berechtigen. Nach der Abberufung als betrieblicher Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

(7) Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem betrieblichen Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen in angemessenem Umfang zu ermöglichen und deren Kosten zu übernehmen.

(8) Im Übrigen findet § 16 entsprechende Anwendung.

(9) Sind mit der automatisierten Datenerhebung, -verarbeitung oder -nutzung weniger als elf Personen befasst, kann die Erfüllung der Aufgaben des betrieblichen Datenschutzes in anderer Weise geregelt werden.

§ 21
Aufgaben des betrieblichen Datenschutzbeauftragten

(1) Der betriebliche Datenschutzbeauftragte wirkt auf die Einhaltung dieser Anordnung und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann er sich in Zweifelsfällen an den Diözesandatenschutzbeauftragten gemäß § 16 KDO wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieser Anordnung sowie anderer Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem betrieblichen Datenschutzbeauftragten ist von der verantwortlichen Stelle eine Übersicht nach § 3a Abs. 2 zur Verfügung zu stellen.

(3) Der betriebliche Datenschutzbeauftragte macht die Angaben nach § 3a Abs. 2 Nr. 1 bis 7 auf Antrag jedermann in geeigneter Weise verfügbar, der ein berechtigtes Interesse nachweist.

§ 22
Ermächtigungen

Die zur Durchführung dieser Anordnung erforderlichen Regelungen trifft der Generalvikar. Er legt insbesondere fest:

a) den Inhalt der Meldung gemäß § 3a,

b) den Inhalt der schriftlichen Verpflichtungserklärung gemäß § 4 Satz 2,

c) die technischen und organisatorischen Maßnahmen gemäß § 6 Satz 1,

d) die Erfüllung der Aufgaben des betrieblichen Datenschutzes gemäß § 20 Abs. 9.

§ 23
Schlussbestimmung

Diese Anordnung tritt am ..... in Kraft.

Gleichzeitig tritt die Anordnung über den kirchlichen Datenschutz – KDO vom ..... außer Kraft.

3. Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (DVO/KDO)

i.d.F. des Beschlusses der Kommission für Meldewesen und Datenschutz vom 25./26. Februar 2003

Aufgrund des § 19 der Anordnung über den kirchlichen Datenschutz (KDO) vom ..... werden mit Wirkung vom ..... die folgenden Regelungen getroffen:

I. Zu § 3a KDO (Meldung von Verfahren automatisierter Verarbeitung)

(1) Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind diese vor Inbetriebnahme schriftlich dem Diözesandatenschutzbeauftragten zu melden. Sofern ein betrieblicher Datenschutzbeauftragter bestellt ist, ist diesem gem. § 18b Abs. 2 KDO eine Übersicht nach § 3a Abs. 2 KDO zur Verfügung zu stellen.

(2) Für die Meldung von Verfahren automatisierter Verarbeitung vor Inbetriebnahme beziehungsweise die dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellende Übersicht soll das Muster gemäß der Anlage verwandt werden.

II. Zu § 4 KDO

(1) Zum Kreis der bei der Datenverarbeitung tätigen Personen im Sinne des § 4 KDO gehören die in den Stellen gem. § 1 Abs. 2 KDO gegen Entgelt beschäftigten und ehrenamtlich tätigen Personen. Sie werden belehrt über:

1. den Inhalt der KDO und anderer für ihre Tätigkeit geltender Datenschutzvorschriften; dies geschieht durch Hinweis auf die für den Aufgabenbereich des Mitarbeiters wesentlichen Grundsätze und im Übrigen auf die Texte in der jeweils gültigen Fassung. Diese Texte werden zur Einsichtnahme und etwaigen kurzfristigen Ausleihe bereitgehalten; dies wird dem Mitarbeiter bekannt gegeben,
2. die Verpflichtung zur Beachtung der in Nummer 1 genannten Vorschriften bei ihrer Tätigkeit in der Datenverarbeitung,
3. mögliche disziplinarrechtliche bzw. arbeitsrechtliche/ rechtliche Folgen eines Verstoßes gegen die KDO und andere für ihre Tätigkeit geltende Datenschutzvorschriften,
4. das Fortbestehen des Datengeheimnisses nach Beendigung der Tätigkeit bei der Datenverarbeitung.

(2) Über die Beachtung der Verpflichtung ist von den bei der Datenverarbeitung tätigen Personen eine schriftliche Erklärung nach näherer Maßgabe des Abschnittes III abzugeben. Die Urschrift der Verpflichtungserklärung wird zu den Personalakten der bei der Datenverarbeitung tätigen Personen genommen, welche eine Ausfertigung der Erklärung erhalten.

(3) Die Verpflichtung auf das Datengeheimnis erfolgt durch den Dienstvorgesetzten der in der Datenverarbeitung tätigen Personen oder einen von ihm Beauftragten.

III. Zu § 4 KDO

(1) Die schriftliche Verpflichtungserklärung der bei der Datenverarbeitung tätigen Personen gemäß § 4 Satz 2 KDO hat zum Inhalt,

1. Angaben zur Identifizierung (Vor- und Zuname, Geburtsdatum und Anschrift sowie Beschäftigungsdienststelle),
2. die Bestätigung, dass auf die für den Aufgabenbereich des Mitarbeiters wesentlichen Grundsätze und im Übrigen auf die Texte in der jeweils gültigen Fassung sowie auf die Möglichkeit der Einsichtnahme und etwaigen kurzfristigen Ausleihe dieser Texte hingewiesen wurde,
3. die Verpflichtung, die KDO und andere für ihre Tätigkeit geltende Datenschutzvorschriften in der jeweils gültigen Fassung sorgfältig einzuhalten,
4. die Bestätigung, dass sie über disziplinarrechtliche bzw. arbeitsrechtliche Folgen eines Verstoßes gegen die KDO belehrt wurden.

(2) Die schriftliche Verpflichtungserklärung ist von der bei der Datenverarbeitung tätigen Person unter Angabe des Ortes und des Datums der Unterschriftsleistung zu unterzeichnen.

(3) Für die schriftliche Verpflichtungserklärung ist das Muster gemäß der Anlage zu verwenden.

IV. Anlage zu § 6 KDO

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maß-

nahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

V. Zu § 12 Abs. 3 KDO

(1) Die Unterrichtung des Betroffenen (§ 2 Abs. 1 KDO) über eine Übermittlung gem. § 12 Abs. 3 Satz 1 KDO erfolgt schriftlich.

(2) Sie enthält

1. die Bezeichnung der übermittelnden Stelle einschließlich der Anschrift,
2. die Bezeichnung des Dritten, an den die Daten übermittelt werden, einschließlich der Anschrift,
3. die Bezeichnung der übermittelten Daten.

VI. Zu § 13 Abs. 1 KDO

(1) Der Antrag des Betroffenen (§ 2 Abs. 1 KDO) auf Auskunft ist schriftlich an die verantwortliche Stelle (§ 2 Abs. 8 KDO) zu richten oder dort zu Protokoll zu erklären.

(2) Der Antrag soll die Art der personenbezogenen Daten, über die Auskunft begehrt wird, näher bezeichnen. Der Antrag auf Auskunft über personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, muss Angaben enthalten, die das Auffinden der Daten ermöglichen.

(3) Der Antrag kann beschränkt werden auf Auskunft über

1. die zur Person des Betroffenen gespeicherten Daten oder

2. die Herkunft dieser Daten oder
3. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben worden sind oder
4. den Zweck, zu dem diese Daten gespeichert sind.

(4) Vorbehaltlich der Regelung in § 13 Abs. 3 KDO wird die Auskunft in dem beantragten Umfang von der verantwortlichen Stelle (§ 2 Abs. 8 KDO) schriftlich erteilt.

(5) Wenn die Erteilung der beantragten Auskunft gemäß § 13 Abs. 2 oder 3 KDO zu unterbleiben hat, so ist dies dem Antragsteller schriftlich mitzuteilen. Die Versagung der beantragten Auskunft soll begründet werden. Für den Fall, dass eine Begründung gem. § 13 Abs. 4 KDO nicht erforderlich ist, ist der Antragsteller darauf hinzuweisen, dass er sich an den Diözesandatenschutzbeauftragten wenden kann; die Anschrift des Diözesandatenschutzbeauftragten ist ihm mitzuteilen.

VII. Zu § 13 a KDO

(1) Die Benachrichtigung des Betroffenen (§ 2 Abs. 1 KDO) gem. § 13a Abs. 1 KDO erfolgt, soweit die Pflicht zur Benachrichtigung nicht nach § 13a Abs. 2 und 3 entfällt, schriftlich durch die verantwortliche Stelle.

(2) Sie enthält

1. die zur Person des Betroffenen gespeicherten Daten,
2. die Bezeichnung der verantwortlichen Stelle,
2. den Zweck, zu dem die Daten erhoben, verarbeitet oder genutzt werden,
3. die Empfänger oder Kategorien von Empfängern, soweit der Betroffene nicht mit der Übermittlung an diese rechnen muss.

VIII. Zu § 14 KDO

(1) Der Betroffene (§ 2 Abs. 1 KDO) kann schriftlich beantragen, ihn betreffende personenbezogene Daten zu berichtigen oder zu löschen. Der Antrag ist schriftlich an die Stellen gem. § 1 Abs. 2 Nr. 2 und 3, im Falle des § 1 Abs. 2 Nr. 1 an das Bistum zu richten.

(2) In dem Antrag auf Berichtigung sind die Daten zu bezeichnen, deren Unrichtigkeit behauptet wird. Der Antrag muss Angaben über die Umstände enthalten, aus denen sich die Unrichtigkeit der Daten ergibt.

(3) In dem Antrag auf Löschung sind die personenbezogenen Daten zu bezeichnen, deren Speicherung für unzulässig gehalten wird. Der Antrag muss Angaben über die Umstände enthalten, aus denen sich die Unzulässigkeit der Speicherung ergibt.

(4) Die zuständige Stelle entscheidet schriftlich über Anträge gem. Abs. 1. Die Entscheidung ist dem Antragsteller bekannt zu geben. Im Falle des § 14 Abs. 7 KDO sind ihm die Stellen anzugeben, die von der Berichtigung, Löschung oder Sperrung verständigt worden sind. Ist eine Verständigung aufgrund des § 14 Abs. 7 KDO unterblieben, sind dem Antragsteller die Gründe dafür mitzuteilen.

(5) Der Widerspruch gemäß § 14 Abs. 5 KDO ist schriftlich oder zur Niederschrift bei der verantwortlichen Stelle (§ 2 Abs. 8 KDO) einzulegen. Die Umstände, aus denen sich das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation ergibt, sind von dem Betroffenen darzulegen. Die verantwortliche Stelle entscheidet über den Widerspruch in geeigneter Form. Die Entscheidung ist dem Betroffenen bekannt zu geben.

Anlagen

1. Zu Abschnitt I. KDO-DVO (§ 3 a KDO Meldung von Verfahren automatisierter Verarbeitungen)

Die Notwendigkeit für die in den nachfolgenden Formularen (Muster 1 und Muster 2) geforderten Angaben ergibt sich aus § 3a KDO. Für jedes automatisierte Verfahren einer verantwortlichen Stelle füllt der Rechtsträger (§ 1 Abs. 2 KDO) ein Formular nach Muster 1 und Muster 2 aus.

Muster 1

Allgemeine Angaben (§ 3a Abs.2 Nr. 1 und Nr. 2 KDO)

1. Name und Anschrift

1.1 des Rechtsträgers (§ 1 Abs. 2 KDO) *(z. B. Kirchengemeinde)*

1.2 der verantwortlichen Stelle (jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt [§ 2 Abs. 8 KDO]) *(z. B. Kindergarten der Kirchengemeinde)*

2. Vertretung der verantwortlichen Stelle

2.1 der nach der Verfassung (Statut, Geschäftsordnung, Satzung) berufene Leiter der verantwortlichen Stelle *(z. B. Leiterin des Kindergartens der Kirchengemeinde)*

2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen *(z. B. beauftragte Gruppenleiterin im Kindergarten der Kirchengemeinde)*

Besondere Angaben (§ 3a Abs.2 Nr. 3 bis Nr. 7 KDO)

3. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung *(z. B. Mitglieder- und Bestandspflege)*

4. Betroffene Personengruppen und Daten oder Datenkategorien

4.1 Beschreibung der betroffenen Personengruppen *(z. B. Arbeitnehmer, Gemeindemitglieder, Patienten usw.)*

4.2 Beschreibung der diesbezüglichen Daten oder Datenkategorien *(Mit „Daten“ sind „personenbezogene Daten“ i. S. d. § 2 Abs. 1 KDO gemeint, wie z. B. Name, Anschrift, Geburtsdatum, Religionszugehörigkeit. Grundsätzlich reicht jedoch die Angabe von Datenkategorien, z. B. Personaldaten, aus. So genannte „besondere Arten personenbezogener Daten“ (vgl. § 2 Abs. 10 KDO) sind entsprechend anzugeben.)*

5. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können (jede Person oder Stelle, die Daten erhält [§ 2 Abs. 9 KDO]) *(z. B. Behörden, kirchliche Stellen, Versicherungen, ärztliches Personal usw.)*.

6. Regelfristen für die Löschung der Daten

7. Geplante Datenübermittlung ins Ausland

_____

Ort, Datum, Unterschrift

Muster 2

Allgemeine Angaben (§ 3a Abs.2 Nr. 1 und Nr. 2 KDO)

1. Name und Anschrift

1.1 des Rechtsträgers (§ 1 Abs. 2 KDO) *(z. B. Kirchengemeinde)*

1.2 der verantwortlichen Stelle (jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt [§ 2 Abs. 8 KDO]) *(z. B. Kindergarten der Kirchengemeinde)*

2. Vertretung der verantwortlichen Stelle

2.1 der nach der Verfassung (Statut, Geschäftsordnung, Satzung) berufene Leiter der verantwortlichen Stelle *(z. B. Leiterin des Kindergartens der Kirchengemeinde)*

2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen *(z. B. beauftragte Gruppenleiterin im Kindergarten der Kirchengemeinde)*

Besondere Angaben (§ 3a Abs.2 Nr. 8 und Nr. 9 KDO)

3. Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (z. B. Konfigurationsübersicht, Netzwerkstruktur, Betriebs- und Anwendungssoftware, spezielle Sicherungssoftware usw.)

4. Zugriffsberechtigte Personen

_____

Ort, Datum, Unterschrift

2. Zu Abschnitt III. KDO-DVO (§ 4 Satz 2 KDO)

Verpflichtungserklärung

Ich verpflichte mich,

1. die Anordnung über den kirchlichen Datenschutz – KDO – des Bistums ..... vom ..... sowie die anderen für meine Tätigkeit geltenden Datenschutzregelungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen sorgfältig einzuhalten und bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen hingewiesen wurde. Ich wurde ferner darauf hingewiesen, dass die KDO und die Texte der übrigen für meine Tätigkeit geltenden Datenschutzvorschriften bei ..... eingesehen und auch für kurze Zeit ausgeliehen werden können,

2. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten.

Ich bin darüber belehrt worden, dass ein Verstoß gegen das Datengeheimnis gleichzeitig einen Verstoß gegen die Schweigepflicht darstellt, der disziplinarrechtliche beziehungsweise arbeitsrechtliche/rechtliche Folgen haben kann.

Diese Erklärung wird zu den Akten genommen.

_____
Vor- und Zuname, Anschrift

_____
Ort, Datum, Unterschrift

4. Einführung in die KDO

(Rechtsanwalt Gerhard Hammer)

Datenschutz
in der Katholischen Kirche/in der Caritas und
in den Katholischen Orden und Gemeinschaften
nach Inkrafttreten der neuen
Anordnung über den kirchlichen Datenschutz (KDO)
von 2003

von Rechtsanwalt Gerhard Hammer
Eltville/Limburg
Geschäftsführer der Kommission
für Meldewesen und Datenschutz des VDD

A. Einleitung

Das Verwaltungshandeln in der katholischen Kirche war bereits in der Vergangenheit immer beherrscht von dem **Grundsatz der besonderen Amtsverschwiegenheit**. Diesem Grundsatz liegt der Gedanke zugrunde, dass die Geheimhaltung kirchlicher Daten, die mit seelsorgerischen Erkenntnissen verbunden sein können, die Regel sein muss und diese nur im Ausnahmefall zur Einsichtnahme Dritten übermittelt werden können. Dabei entspricht es dem überkommenen kirchlichen Selbstverständnis zum Umgang mit persönlichen Daten, selbst dem Betroffenen gegenüber Auskunft nur zu erteilen, soweit der Vertrauensschutz Dritter, das allgemeine kirchliche Interesse oder spezifische kirchliche Bestimmungen oder Interessen dem nicht entgegenstehen.

Dies ist letztlich Folge des **Gedankens des Schutzes der eigenen Intimsphäre**, der bereits in den cc. 220, 223 sowie 983 und 984 des Codex Juris Canonici von 1983 formuliert wurde.

Die Entwicklung der Informationstechnik mit weltweiter Vernetzung und Datenübermittlung und immer neuen Formen der elektronischen Kommunikation ist in den letzten 30 Jahren so rasant vorangeschritten, dass sich der Bundesgesetzgeber und auch die jeweiligen Landesgesetzgeber zu gesetzlichen Regelungen des Datenschutzes veranlasst sahen.

Spätestens seitdem der Erste Senat des Bundesverfassungsgerichtes mit Urteil vom 15.12.1983 in dem so genannten Volkszählungsurteil den Schutz von persönlichen Daten als Teil des allgemeinen Persönlichkeitsrechts erkannt hat, bestand weiterer Handlungsbedarf.

Nach der **europäischen Datenschutzrichtlinie 95/46/EG vom 24.10.1995 (EG-Datenschutzrichtlinie)**, die für den ganzen

europäischen Wirtschaftsraum einheitliche Datenschutzstandards gesichert hat, müssen die Datenschutzgesetze dazu beitragen, das Grundrecht auf informationelle Selbstbestimmung zu verwirklichen.

Die verfassten Kirchen (insbesondere die Katholische Kirche und die Evangelischen Kirchen) verwenden nicht nur eine Vielzahl von Daten, die sie selbst von ihren Mitgliedern oder den von ihnen betreuten Personen erhoben haben. Vielmehr werden ihnen auch zahlreiche Daten vom Staat aufgrund gesetzlicher Ermächtigungen zur Verfügung gestellt.

Dabei fordert der Staat von den Kirchen, dass bei diesen sichergestellt ist, dass „gleichwertige" oder „ausreichende" Datenschutzmaßnahmen vorliegen (vgl. für Hessen: § 35 hess. DatenschutzG und im Bund: § 15 Abs. 4 BDSG).

Obwohl die Katholischen Bistümer in erster Linie Daten von Stellen der Kommunal- und Landesverwaltung erhalten, für die **vor** der Übermittlung die jeweiligen unterschiedlichen (Landes-) Datenschutzgesetze gelten, haben sie dennoch auf das **Bundesdatenschutzgesetz als Orientierung** zurückgegriffen, weil die Bistümer meist länderübergreifende Grenzen haben und aus **Gründen der Rechtseinheit** in allen Bistümern der Katholischen Kirche eine bundeseinheitliche Datenschutzregelung anstrebten.

Mit der Neufassung der Anordnung über den Kirchlichen Datenschutz (KDO) haben die Bischöfe der Bundesrepublik Deutschland die Anpassung des Datenschutzes in ihren Bistümern an die geänderte Gesetzeslage vollzogen, die mit dem Inkrafttreten des novellierten **Bundesdatenschutzgesetzes (BDSG) vom 20.12.2001 (BGBl. I S. 3926) in der Fassung der Neubekanntmachung vom 14.01.2003 (BGBl. I S. 66)** entstanden ist.

Die Bischöfe haben dabei jedoch nicht alle Neuerungen des BDSG pauschal übernommen, sondern aufgrund des Rechtes der Katholischen Kirche, ihre Angelegenheiten selbst zu regeln, eine **eigene Datenschutzordnung**, die **Anordnung über den kirchlichen Datenschutz (KDO)** erlassen, die den besonderen kirchlichen Anliegen innerhalb des kirchlichen Datenschutzes Rechnung tragen soll.
Dies kommt insbesondere in der **Präambel der KDO** zum Ausdruck.

Ferner nimmt der jeweilige Ortsbischof dieses Recht nicht nur für sich und seine verfasste (Teil-) Kirche in Anspruch, sondern auch für die selbstständigen, zum Teil in privatrechtlicher Form organisierten kirchlichen Einrichtungen.

Darunter fallen auch die Orden bischöflichen Rechts.

Die Bischöfe stützen sich dabei auf die Rechtssprechung des Bundesverfassungsgerichtes wonach die Zugehörigkeit zur Kirche nicht davon abhängt, ob die Einrichtung unmittelbar Teil der verfassten Kirche ist. Voraussetzung ist vielmehr, ob die Einrichtung einen kirchlichen Auftrag hat und organisatorisch in das Wirken der Kirche eingebunden ist (vgl. auch BVerfGE 70, 138, 165 = KirchE 23, 105, 110 m.w.N.).

Mit der Einbeziehung auch der privatrechtlich organisierten Einrichtungen der Kirchen machen die Bischöfe deutlich, dass diese trotz ihrer privatrechtlichen Rechtsform Stellen der öffentlich-rechtlichen Religionsgesellschaft (des jeweiligen Bistums) sind und bleiben.

Kirchliche Einrichtungen, insbesondere in privatrechtlicher Rechtsform, die sich dem Staat und dem Bischof gegenüber auf die (kirchliche) Autonomie berufen wollen, können sich mit dieser Argumentation aber keinen datenschutzrechtlichen Frei-

raum schaffen und fallen grundsätzlich unter die Datenschutzregelung der Kirche zu der sie gehören.

Einrichtungen, die sich selbst als kirchliche Einrichtung verstehen sind daher gehalten, die KDO für ihren Bereich rechtsverbindlich anzuwenden.

Hinsichtlich der **Orden (und der geistlichen Gemeinschaften) gelten folgende Besonderheiten:**

Zunächst muss unterschieden werden, ob es sich im konkreten Fall um einen Orden oder um eine kirchliche Gemeinschaft handelt, die bischöflichem Recht oder päpstlichem Recht unterliegt:

- Für die Orden bischöflichen Rechts, soweit in diesen Fällen eine bischöfliche Aufsichts- und Eingriffsmöglichkeit besteht, sind sie als Stellen der öffentlich-rechtlichen Religionsgesellschaft anzusehen.
- Bei den Orden päpstlichen Rechts ist die Lage anders. Hier muss die zuständige Ordensleitung ausdrücklich die Anordnung über den kirchlichen Datenschutz als eigenes Recht erklären. Hierzu wurde die Ordens-KDO von den „Ordensdachorganisationen“, der Mitgliederversammlung der VOD am 11.06.2003 und der Mitgliederversammlung der VDO und VOB am 30.06.2003 beschlossen.

Aus Beweisführungsgründen sollte die Geltung der KDO für selbständige kirchliche Einrichtungen in Zweifelsfällen immer in einem förmlichen Beschluss und gegebenenfalls in einem Protokoll niedergelegt sein.

Hinsichtlich der Orden wird bei der Vereinigung Deutscher Ordensobern (VDO) ein Register geführt.

B. Die Anordnung über den kirchlichen Datenschutz – KDO von 2003 –

1. Die KDO

Als Folge des kirchlichen Selbstbestimmungsrechtes gem. Artikel 137 Absatz 3 der Weimarer Reichsverfassung vom 11.08.1919 (WRV) in Verbindung mit Artikel 140 Grundgesetz (GG) gibt die (Ordens-)KDO der verfassten Kirche (Bistümern, Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbände), ihren Körperschaften, Stiftungen, Anstalten, Werken, Einrichtungen und sonstigen kirchlichen Rechtsträgern einschließlich der Caritasverbände, ihrer Untergliederungen und ihrer Fachverbände sowie den kirchlichen Orden und Gemeinschaften einen Rahmen, in dem sie ihre Aufgaben unter Beachtung des Persönlichkeitsrechtes Dritter wahrnehmen können.
Sie unterstehen damit unmittelbar einem eigenen, kirchlichen Diözesandatenschutzbeauftragten, dem Ordensdatenschutzbeauftragten (bei Orden päpstlichen Rechts) oder, bei den Orden bischöflichen Rechts, dem Datenschutzbeauftragten des so genannten „Belegenheitsbistums", also dem dortigen Diözesandatenschutzbeauftragten.

Orden und Gemeinschaften **bischöflichen Rechts** mit Niederlassungen in verschiedenen Bistümern müssten pragmatisch klären (lassen), ob sie **einem** Datenschutzbeauftragten unterstehen oder ob dies von dem jeweiligen Diözesandatenschutzbeauftragten des Belegenheitsbistums der Ordensniederlassung wahrgenommen werden kann.

Die Staatskirchenrechtskommission des VDD hat hierzu 1995/ 1996 folgende Empfehlung abgegeben:

Für Einrichtungen eines mehrdiözesanen oder überdiözesanen Rechtsträgers gilt der Rechtssetzungsakt des Diözesanbischofs, in dessen Diözese sich der Sitz der Hauptniederlassung (Hauptsitz) befindet. Abweichend von diesem Grundsatz kann der Diözesanbischof, in dessen Diözese sich die Einrichtung befindet, im Einvernehmen mit dem Diözesanbischof des Hauptsitzes bestimmen, dass die diözesane Ordnung Anwendung findet oder er kann eine Rechtsordnung eigens für den Rechtsträger erlassen.

2. Sicherung des Persönlichkeitsrechts durch die KDO (Ordens-KDO)

2.1 Das Ziel des Datenschutzes

Gesetzesbestimmungen: § 1 KDO, Art. 1 und 2 GG, cc. 220 ff. CIC

Ziel des Datenschutzes ist es, den Menschen vor Gefährdungen durch nachteilige Folgen der Datenverarbeitung zu schützen.

Die Anordnung über den kirchlichen Datenschutz umschreibt ihre Zweckbestimmung in § 1 Absatz 1 KDO wie folgt:

„Zweck dieser Anordnung ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“

Den gleichen Zweck verfolgen Datenschutzvorschriften in anderen Gesetzen (z. B. § 1 Abs. 1 BDSG, § 30 Abgabenordnung – Steuergeheimnis – oder besondere Bestimmungen in den Sozialgesetzbüchern).
Das Persönlichkeitsrecht wird abgeleitet aus den Grundrechten der Verfassung.

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt.“
(Artikel 1 Absatz 1 Grundgesetz) und

„Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung und das Sittengesetz verstößt.“
(Artikel 2 Absatz 1 Grundgesetz)

Diese Verfassungsartikel sind auch Grundlage des kirchlichen Datenschutzes, wobei – wie bereits oben erwähnt – auch der CIC, der Kodex des Kanonischen Rechtes von 1983, von Bedeutung ist. Dort heißt es:

„Niemandem ist es erlaubt, den guten Rufen, den jemand hat, rechtswidrig zu schädigen und das Recht irgendeiner Person auf Schutz der eigenen Intimsphäre zu verletzen.“ (can. 220 CIC)

„Das Beichtgeheimnis ist unverletzlich; dem Beichtvater ist daher streng verboten, den Pönitenten durch Worte oder auf irgendeine andere Weise oder aus irgendeinem Grund irgendwie zu verraten.

Zur Wahrung des Geheimnissen sind auch, falls beteiligt, der Dolmetscher und alle anderen verpflichtet, die auf irgendeine Weise aus der Beichte zur Kenntnis von Sünden gelangt sind.“ (can. 983 § 1 und § 2 CIC)

Darüber hinaus hat das Bundesverfassungsgericht dazu im so genannten Volkszählungsurteil vom 15.12.1983 folgendes festgestellt:

„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Zur Begründung führt das Gericht aus:

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“

Das Recht auf informationelle Selbstbestimmung soll dem Einzelnen ermöglichen, sich seine Privatsphäre zu erhalten, und zu verhindern, dass er deshalb in zunehmender Abhängigkeit von Stellen in Staat, Wirtschaft und Verwaltung gerät, weil diese immer mehr von ihm wissen.

Allerdings braucht der moderne Rechts- und Sozialstaat und auch die Kirche in großem Umfang personenbezogene Daten, um seine/ihre vielfältigen Aufgaben fachlich richtig und gerecht erfüllen zu können.

So können zum Beispiel im staatlichen Bereich Sozialämter, Schulen, Kindergärten, Steuerbehörden und die Polizei ihre

Aufgaben nicht ordentlich erfüllen, wenn sie allein auf die freiwillige Mitwirkung der Menschen angewiesen wären.

Die Kirchengemeinden können nicht zu Seniorennachmittagen oder zur Kinderkatechese einladen, wenn sie nicht bestimmte Altersgruppen aus den Meldedaten auswählen können. Auch betreibt die Kirche Schulen, Kindergärten, Krankenhäuser und andere soziale Einrichtungen, bei denen eine Vielzahl von personenbezogenen Daten erhoben, verarbeitet und genutzt werden.

Bei den Orden geht es auch um Daten, die sie über ihre Mitglieder oder derzeitige und ehemalige Zöglinge gespeichert haben.

Bei Gemeinschaften mit Tätigkeiten in den Bereichen Kindergarten, Schule/Hochschule, Internat, Hort, Tagesheim, Jugendfürsorge, etc. werden verschiedene personenbezogene Daten anfallen, um Abrechnungen und sonstige Verwaltungsaufgaben damit vor zu nehmen.

Auch werden Daten von Patienten und zu betreuenden Personen bei Gemeinschaften mit Tätigkeiten in den Bereichen Krankenhaus, Alten- und Behindertenpflege, Behindertenwerkstätten, etc. gespeichert.

Schließlich werden Daten von Spendern und Wohltätern, Freunden und Förderern und nicht zu vergessen: Kundendaten und Firmendaten bei wirtschaftlichen Geschäftsbetrieben von Orden, Gemeinschaften und Klöstern erhoben, verarbeitet und genutzt.

Teilweise gibt es die (gesetzliche) Verpflichtung diese Daten zu speichern und aktuell zu halten.

Das Recht auf informationelle Selbstbestimmung kann deshalb nicht schrankenlos sein. Das hat auch das Bundesverfassungsgericht festgestellt, zugleich aber eindeutige Grenzen für Einschränkungen dieses Rechts bestimmt:

Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur aufgrund eines Gesetzes zulässig.

Das Gesetz muss

- im überwiegenden Allgemeininteresse erforderlich sein,
- die Voraussetzung für die Einschränkung des Grundrechts und dessen Umfang für den Bürger erkennbar regeln, also dem Gebot der Normklarheit entsprechen und
- den Grundsatz der Verhältnismäßigkeit beachten.

Wenn Gesetze in das Recht auf informationelle Selbstbestimmung des Einzelnen eingreifen, muss der Gesetzgeber folgende Punkte beachten:

- Nur das erforderliche Minimum an Daten darf verlangt werden,
- die Daten dürfen grundsätzlich nur für den Zweck verwendet werden, für den sie erhoben oder erfasst wurden.
- Der Gesetzgeber muss durch ergänzende Vorkehrungen dafür sorgen, dass auch bei der Organisation und beim Verfahren des Umgangs mit personenbezogenen Daten auf die Rechte des Einzelnen Rücksicht genommen wird (z. B. durch Mitwirkungs- und Kontrollrechte).

Das Recht auf den Schutz personenbezogener Daten wurde auch in Artikel 8 der Charta der Grundrechte der Europäischen Union aufgenommen. Die Charta ist jedoch nicht rechtsverbindlicher Bestandteil der europäischen Verträge.

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr gibt in Artikel 1 Absatz 1 den Mitgliedstaaten vor, nach den Bestimmungen der Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

Die Novellierung des Bundesdatenschutzgesetzes im Jahre 2001 (in der Fassung von 2003) diente unter anderem der Umsetzung der Richtlinie in deutsches Recht.

Wie oben bereits schon erwähnt haben die deutschen Bischöfe auf das Bundesdatenschutzgesetz als Orientierung zurückgegriffen und die einzelnen Formulierungen unter Berücksichtigung von kirchlichen Besonderheiten übernommen.

2.2 Rahmenbedingungen für einen wirksamen Datenschutz

Die KDO stellt allgemeine datenschutzrechtliche Grundregeln auf. Diese Grundregeln passen allerdings nicht überall und sie sind nicht überall ausreichend.

Man braucht nur etwa an die verschiedenen Bereiche denken, bei denen die verfasste Kirche, ihre privatrechtlich organisierten kirchlichen Einrichtungen oder Orden und christliche Gemeinschaften beispielsweise im Gesundheitswesen arbeiten. So haben beispielsweise die Arbeitsgemeinschaft der Katholischen Krankenhäuser in Hessen, Rheinland-Pfalz und dem Saarland eine Ordnung zum Schutz von Patientendaten in Katholischen Krankenhäusern entwickelt, die von den verschiedenen Bistümern in Kraft gesetzt worden sind. Ferner gibt es Spezialrege-

lungen in anderen Gesetzen wie z. B. dem Sozialgesetzbuch, dem Melderechtsrahmengesetz, aber auch in der Abgabenordnung.

Manche Bistümer haben als Träger von Schulen auch Datenschutzbestimmungen für ihre Schulen erlassen.

Diese so genannten **bereichsspezifischen Regelungen** gehen der KDO vor, so wie die bereichsspezifischen Regelungen im staatlichen Bereich dem Bundes- und den Landes-Datenschutzgesetzen vorgehen.

Es ist daher notwendige Konsequenz, dass die Kirche beispielsweise hinsichtlich des Melderechtsrahmengesetzes eine eigene Anordnung über das kirchliche Meldewesen entwickelt oder im Bereich des Sozialgesetzbuches eigene Regelungen trifft, beziehungsweise getroffen hat.

Schließlich haben die Bischöfe zum Schutz des Schrift- und Dokumentationsgutes ihres Verantwortungsbereiches noch Anordnungen über die Sicherung und Nutzung der Archive der Katholischen Kirche in ihrem (Erz-) Bistum erlassen, in denen Nutzungsvoraussetzungen, Sperrfristen und Zugangsberechtigungen geregelt sind.

Die bereichsspezifischen Regelungen reichen aber in einer vernetzten Welt mit einer rasanten Entwicklung im Bereich der Informationstechnologie, in der überall Daten gesammelt werden, nicht immer aus.
Nach Einschätzung vieler muss der rechtliche Rahmen zwar sein, es müssen aber noch eine Vielzahl verschiedenster Maßnahmen hinzukommen.

So müssen Maßnahmen der rechtsausfüllenden Selbstregulierung durch die Anwender, Selbstschutzvorkehrungen des Einzelnen, vor allem aber der Einsatz datenvermeidender und datensparsamer Technik ineinander greifen.

Die KDO trägt zur Sicherung des Datenschutzes bei, in dem sie Regelungen für den Umgang mit personenbezogenen Daten aufstellt.

Dabei geht die KDO davon aus, dass jegliche Verarbeitung von personenbezogenen Daten einer ausdrücklichen Erlaubnis bedarf,

- sei es über ein Gesetz oder
- über eine ausdrücklich erteilte Einwilligung des Einzelnen.

Sie enthält Schutzregelungen für das informelle Selbstbestimmungsrecht bezüglich der Datenverarbeitung, die die Datenverarbeiter und Anwender zu beachten haben.

Diese begründen spiegelbildlich auch die Rechte der von der Datenverarbeitung betroffenen Bürgerinnen und Bürger.

Die KDO verpflichtet die Datenverarbeiter also von vorn herein, die rechtlichen „Spielregeln“ der Datenverarbeitung zu beachten, die Betroffenen in bestimmten Fällen zu informieren und zu benachrichtigen.
Sie weist aber auch den Betroffenen eine Reihe von Rechten ausdrücklich zu.

Dabei setzt die KDO bereits bei der Vorbeugung an. Vorrangiges Ziel des Datenschutzes ist es, eine Gefährdung des Persönlichkeitsrechts des Einzelnen von vornherein zu verhindern, durch Aufstellen von Regeln und die Nutzbarmachung der Technik.

„Datenschutzfreundliche Technik“ soll eingesetzt werden, um möglichst ohne personenbezogene Daten, oder – wo das nicht möglich ist – mit so wenig wie möglich personenbezogenen Daten auszukommen.

Riesige Datenmengen sollen erst gar nicht entstehen.
Die technischen und organisatorischen Maßnahmen, die nach § 6 KDO und seiner dazu ergangenen Anlage zu treffen sind, sollen dann die Datenverarbeitung über Organisationen und Einsatz von Technik sichern.

Eine besonders wichtige Rolle haben auch die Datenschutzbeauftragten inne. Ihre Aufgabe ist es, auf die Sicherung des Datenschutzes hinzuwirken. Sie sind wichtige Ansprechpartner für Betroffene sowie für die Beschäftigten ihrer Organisationen.

Die neue KDO ermöglicht im Zusammenwirken von Verwaltung und Datenschutzbeauftragten neue Perspektiven für selbst regulierte Schutzmaßnahmen im Datenschutz.

2.3 Der Anwendungsbereich der KDO

Gesetzesbestimmung: § 1 Abs. 2 KDO

Die KDO gilt uneingeschränkt für die in Absatz 2 genannten Stellen.

Auch die (Ordens-)KDO trifft hier eine klare Aussage. Sie gilt für die Ordensgemeinschaften und Klöster päpstlichen Rechts.

Die KDO gilt aber nur, soweit es keine besonderen kirchlichen oder staatlichen Rechtsvorschriften gibt, die auf personenbezogene Daten einschließlich der Veröffentlichung anzuwenden sind. Auch die Verpflichtung zur Wahrung des Beicht-/Seelsor-

gegeheimnisses, andere gesetzliche Geheimhaltungspflichten oder von anderen Berufs- oder besonderen Amtsgeheimnissen, die auf gesetzlichen Vorschriften beruhen, bleiben unberührt. Hierunter fallen beispielsweise die oben bereits angesprochenen Bestimmungen im Codex Juris Canonici (CIC) zum Beichtgeheimnis, hierunter fällt auch das Steuergeheimnis, dass in § 30 Abgabenordnung (AO) eine besondere Regelung erfährt.

Wichtig ist, dass die KDO auch für Daten in Akten und anderen Unterlagen gilt. Allerdings sind die kirchlichen Geheimakten davon ausgenommen. Diese werden aber besonders geschützt und dürfen nur von einer äußerst begrenzten Anzahl von Personen eingesehen werden.

2.4 Verbot mit Erlaubnisvorbehalt

Gesetzesbestimmungen: § 9 und § 10 KDO

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein so genanntes Verbot mit Erlaubnisvorbehalt. Das heißt:

Grundsätzlich ist verboten, was nicht ausdrücklich erlaubt ist!

Das bedeutet, die Erhebung, Verarbeitung und Nutzung von Daten sind verboten, es sei denn,

- sie sind durch die KDO oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet
- oder der Betroffene hat dazu seine Einwilligung erklärt.

Wenn eine Rechtsvorschrift den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die Einwilligung des Betroffenen nicht an.

Soll eine Einwilligung Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, ist zu beachten:

- die **Einwilligung bedarf der Schriftform**, soweit nicht wegen besonderen Umständen eine andere Form angemessen ist,
- der **Betroffene ist vorher über die Tragweite seiner Einwilligung aufzuklären** (z. B. über den Zweck der Erhebung, Verarbeitung oder Nutzung); soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen ist er auch darüber zu informieren, was geschieht, wenn er nicht einwilligt (z. B. das Ansprüche verloren gehen können).

Die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen; d. h. sie muss frei von Zwang sein. In diesem Zusammenhang ist auch zu berücksichtigen, ob sich der Betroffene in einer besonderen Situation (z. B. Arbeitsverhältnis) befindet oder ob aufgrund einer faktischen Situation (beispielsweise Monopolstellung desjenigen, der die Einwilligung einholen will) ein Zwang besteht.

Bei der Verarbeitung **besonderer Arten personenbezogener Daten** gem. § 9 Abs. 3 und § 10 Abs. 5 (Angaben über die rassische oder ethnische Herkunft, politische Meinung, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) muss sich die Einwilligung ausdrücklich auf diese Daten beziehen. Nicht beziehen muss sich die Einwilligung auf die (bloße) Angabe der Zugehörigkeit zu einer Kirche oder sonstigen Religionsgemeinschaft (§ 2 Abs. 10 Satz 2).

Bei dieser Regelung wurde insbesondere Artikel 140 GG in Verbindung mit Artikel 136 Abs. 3 der Verfassung vom

11.08.1919 – WRV – bedacht, wonach zwar niemand verpflichtet ist, seine religiöse Überzeugung zu offenbaren, aber die Zugehörigkeit zu einer Religionsgemeinschaft erfragt werden darf.

2.5 Der Zweckbindungsgrundsatz

Gesetzesbestimmung: § 10 Abs. 2 KDO

Die Speicherung, Veränderung und Nutzung personenbezogener Daten durch öffentliche Stellen ist zulässig, wenn

- dies zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und
- sie für die Zwecke erfolgt, für die die Daten erhoben worden sind (falls keine Erhebung voranging: für die sie gespeichert worden sind). Hiermit wird der **Zweckbindungsgrundsatz** angesprochen, d. h. das personenbezogene Daten grundsätzlich nur zu den Zwecken verarbeitet werden dürfen, für die sie erhoben bzw. gespeichert worden sind.

Von diesem Grundsatz sieht das Gesetz aber eine Reihe von zum Teil weit reichenden Ausnahmen vor.

Welche Ausnahmen von der Zweckbindung gibt es?

Die Verarbeitung personenbezogener Daten **für einen anderen Zwecke** ist zulässig, wenn

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
- der Betroffene eingewilligt hat,
- es offensichtlich im Interesse des Betroffenen liegt,
- Angaben des Betroffenen überprüft werden müssen, weil begründete Zweifel an ihrer Richtigkeit bestehen,

- die Daten allgemein zugänglich sind, oder veröffentlich werden dürfen (aber nicht, wenn das entgegen stehende schutzwürdige Interesse des Betroffenen offensichtlich überwiegt),

oder wenn sie

- zur Gefahrenabwehr, oder zur Wahrung erheblicher Belastungen des Gemeinwohls erforderlich ist,
- zur Verfolgung von Straftaten oder von Ordnungswidrigkeiten,
- zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte eines anderen oder
- zur Durchführung wissenschaftlicher Forschung (nach näher bestimmten Voraussetzungen) und schließlich erforderlich ist.
- Oder **der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert.**

Diese Regelung soll den kirchlichen Besonderheiten Rechnung tragen und es ermöglichen die von der Kirche definierten Besonderheiten zu berücksichtigen.
Dies gilt übrigens auch für das Erheben besonderer Arten personenbezogener Daten gemäß § 9 Abs. 5 Nr. 6 KDO (vgl. unten 2.6).

Für die zweckändernde Verarbeitung oder Nutzung besonderer Arten personenbezogener Daten gilt eine Sonderregelung. Unter anderem ist danach eine Zweckänderung zulässig, wenn die Daten für den geänderten Zweck erhoben werden dürfen. Sonderregelungen gelten auch für eine zweckändernde Verarbeitung von besonderen personenbezogenen Daten zur Durchführung wissenschaftlicher Forschung bzw. für Zwecke der Gesundheitsvorsor-

ge, medizinische Diagnostik und weiteres (§ 10 Abs. 2 Nr. 9 KDO).

Auf der anderen Seite wird klargestellt, dass eine bestimmte Verwendung von Daten nicht als Zweckänderung anzusehen ist, so die Verwendung für

- die Rechnungsprüfung,
- die Wahrnehmung von Aufsichts- und Kontrollbefugnissen,
- Organisationsuntersuchungen sowie
- Ausbildungs- und Prüfungszwecke der speichernden Stelle, aber nur, soweit nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen (z. B. bei persönlichen Angaben) (§ 10 Abs. 3 KDO).

Eine strikte Zweckbindung besteht für Daten, die ausschließlich gespeichert werden zu Zwecken

- der Datenkontrolle,
- der Datensicherung,
- der Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage oder
- der wissenschaftlichen Forschung.

Erforderlich ist stets eine Abwägung nach Maßgabe des Gesetzes zwischen den entgegenstehenden schutzwürdigen Interessen des Betroffenen und dem Interesse der verantwortlichen Stelle an der Zweckänderung.

2.6 Die Datenerhebung

Gesetzesbestimmungen: §§ 3, 8 und 9 KDO

Die Erhebung von Daten ist ebenfalls von den Zulässigkeitsregelungen für die Datenverarbeitung umfasst.

Die Datenerhebung darf nur in dem erforderlichen Umfang erfolgen.

Maßgebend für die Datenerhebung sind der Vertrag oder die Geschäftsbeziehung und dessen Zweck.

- Die Datenerhebung kann auch erforderlich sein zur Wahrung berechtigter Interessen der verantwortlichen Stelle. Hier darf kein Grund zu der Annahme bestehen, dass **schutzwürdige Interessen des Betroffenen** an dem Ausschluss der Verarbeitung oder Nutzung das Interesse der verantwortlichen Stelle an der Datenerhebung überwiegen.

- Auch wenn Daten **allgemein zugänglich** sind oder veröffentlicht werden dürfen, können sie für eigene Geschäftszwecke erhoben werden, es sei denn, schutzwürdige Interessen des Betroffenen würden gegenüber den berechtigten Interessen der verantwortlichen Stellen offensichtlich überwiegen.

- **Besondere Arten personenbezogener Daten** (Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse und philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) dürfen – **ohne wirksame Einwilligung des Betroffenen** – nur in vom Gesetz abschließend aufgeführten Ausnahmefällen erhoben werden.

Zum Beispiel gilt dies:

- zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten,
- bei Daten, die der Betroffene offenkundig öffentlich gemacht hat,

- für wissenschaftliche Forschungszwecke nach Güterabwägung
- und in weiteren im einzelnen aufgeführten Ausnahmetatbeständen,
- **wenn der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erforderlich macht.**

Bei der Datenverarbeitung wird häufig die Ausnahme greifen, die das Erheben besonderer Arten personenbezogener Daten erlaubt, soweit eine Rechtsvorschrift dies vorsieht **oder aus Gründen eines** wichtigen öffentlichen Interesses oder **eines kirchlichen Interesses dies zwingend erfordert.**

Die Daten sind grundsätzlich beim Betroffenen zu erheben. Es ist ihm mitzuteilen, zu welchem Zweck dies geschieht. Nur in Ausnahmefällen dürfen die Daten bei anderen und ohne Kenntnis des Betroffenen erhoben werden.

Ist der Betroffene gegenüber einer öffentlichen Stelle zur Auskunft verpflichtet (z. B. bei amtlichen Statistiken oder Meldebehörden), so muss ihm gesagt werden, nach welchen Rechtsvorschriften das der Fall ist.
Er ist auch aufzuklären, wenn er ohne die von ihm verlangten Auskünfte seine Ansprüche nicht durchsetzen kann oder ihm sonstige Rechtsvorteile entgehen.

Anderenfalls muss dem Betroffenen gesagt werden, dass die Auskunft freiwillig ist.

Ausnahmen:
Ohne Mitwirkung des Betroffenen (z. B. durch Anfragen bei Behörden oder anderen Stellen seien sie kirchlicher oder staatlicher Art) dürfen Daten nur erhoben werden, wenn

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
- die zu erfüllende Verwaltungsaufgabe **ihrer Art nach** eine Erhebung **bei anderen Personen** oder Stellen erforderlich macht und keine Beeinträchtigung überwiegender schutzwürdiger Interessen des Betroffenen zu erwarten ist,
- die Erhebung beim Betroffenen einen **unverhältnismäßig hohen Aufwand** zur Folge hätte (z. B. weil er schwer zu finden ist) und auch hier keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Ob die befragte Stelle die erbetenen Daten übermitteln darf, muss diese aber besonders prüfen.

Wenn die personenbezogenen Daten beim Betroffenen erhoben werden, so muss er, wenn er nicht bereits auf andere Weise Kenntnisse hat, **informiert** werden. Er hat Anspruch darauf zu erfahren,

- welche die verantwortliche Stelle ist, die die Daten erhoben hat,
- welche die Zweckbindung für die erhobenen Daten ist,
- und ggf. auch, welche Kategorien von Empfängern der Daten sind, sofern er nach den Umständen des Einzelfalls nicht mit einer Übermittlung an diese rechnen muss.

Nur so ist gewährleistet, dass der Betroffene seine Datenschutzrechte wahrnehmen kann.

Werden die Daten ohne Mitwirkung des Betroffenen erhoben, so ist § 13a KDO anzuwenden.

2.7 Die Übermittlung von Daten

Gesetzesbestimmungen: §§ 11 und 12 KDO

Die KDO kennt unterschiedliche Regelungen je nach dem ob es sich um eine Datenübermittlung an kirchliche und öffentliche Stellen handelt oder um eine Datenübermittlung an nichtkirchliche und nichtöffentliche Stellen.
Eine besondere Regelung gilt für die Datenübermittlung an eine kirchliche oder öffentliche Stelle im **Ausland.**
Eine Datenübermittlung an nichtkirchliche und nichtöffentliche Stellen im Ausland ist nicht vorgesehen. Bei der Übermittlung personenbezogener Daten an öffentliche Stellen oder an kirchliche Stellen außerhalb des Geltungsbereiches der KDO ist die Übermittlung zulässig, wenn

- es für die Aufgabenerfüllung der übermittelnden Stelle oder des Dritten an den die Daten übermittelt werden, erforderlich ist und
- der Verwendungszeck beim Dritten, an den die Daten übermittelt werden, gleich ist oder eine zulässige Zweckänderung vorliegt.

Wann ist die Übermittlung ins Ausland zulässig?

Gesetzesbestimmung: § 11 Abs. 4 KDO

Für die Datenübermittlung ins Ausland gilt eine besondere Regelung. Gemäß § 11 Abs. 4 KDO muss sichergestellt sein, dass neben den Voraussetzungen in den Absätzen 1 bis 3 **bei dem Empfänger ausreichende Datenschutzmaßnahmen** getroffen werden.

Ob in einem Land ein angemessenes Datenschutzniveau besteht, kann festgestellt werden, durch die verantwortliche Stelle selbst, die die Daten übermitteln will, nach den Kriterien

- Art der Daten,
- Zweckbestimmung,
- Dauer der geplanten Verarbeitung,
- Herkunft und Bestimmungsland,
- für den Empfänger geltende Rechtsnormen,
- Standesregeln und Sicherheitsmaßnahmen.

Dabei ist die Datenübermittlung in ein Land innerhalb der europäischen Union und mit den anderen Vertragsdaten des Abkommens über den europäischen Wirtschaftsraum prinzipiell genauso zu behandeln wie der inländische Wirtschaftsraum.

Ein Sonderweg wurde für den Datenverkehr mit den USA geschaffen. Es handelt sich um die so genannten „Safe Harbor Principles“, kurz „safe harbor“ („sicherer Hafen“) genannt.

Die nach nationalem (deutschem) Recht zulässige Datenübermittlung ist danach als Datenübermittlung in die USA zulässig, sofern sich der dortige Empfänger freiwillig den Regelungen von „safe harbor“ unterworfen hat.

Diese Verfahrensweise könnte aber aufgrund der neueren Rechtsprechung des EuGH in nächster Zeit durch gesetzgeberische Maßnahmen möglicherweise für die Zukunft abgeändert werden. Die weitere Entwicklung sollte daher beachtet werden.

Ausnahmen:
Darüber hinaus kommt eine Übermittlung an einen Drittstaat auch im Rahmen weit reichender Ausnahmeregelungen unter Umständen in Betracht. Bedeutsam ist auch die Genehmigung

der Übermittlung durch die zuständige Datenschutzaufsichtsbehörde gemäß § 4c Abs. 2 BDSG.

Wie sich dies bei Orden und kirchlichen Gemeinschaften verhält, die Rechtsbeziehungen nach Afrika und Südamerika oder Asien unterhalten, kann von hier aus nicht abschließend beantwortet werden und müsste ggf. über das Auswärtige Amt in Erfahrung gebracht werden.

Grundsätzlich ist es aber so, dass immer dann, wenn gleichwertige Datenschutzmaßnahmen beim Empfänger getroffen wurden, und dies wird bei Ordensniederlassungen im Ausland in der Regel anzunehmen sein, auch eine Übermittlung zulässig ist.

2.8 Die technischen und organisatorischen Maßnahmen

Gesetzesbestimmung: § 6 KDO

Ein sehr wichtiger, oft arbeits- und kostenintensiver Bereich des Datenschutzes sind die technischen und organisatorischen Maßnahmen für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, die getroffen werden müssen, damit diese vor Missbrauch, Fehlern und Unglücksfällen möglichst sicher sind.

Welche Maßnahmen notwendig sind, hängt nicht nur von der Art der Daten ab, sondern ebenso von der Aufgabe, den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen.

Die KDO verzichtet deshalb darauf, bestimmte einzelne Maßnahmen zwingend vorzuschreiben, sondern verlangt nur allgemein,

„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."

Welche Wirkung diese Maßnahmen im Bereich der automatisierten Verarbeitung haben müssen, legt die KDO in Form der Anlage zu § 6 KDO dar.

Ferner ergibt sich aus der Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz eine Meldepflicht von Verfahren automatisierter Verarbeitung. Die Maßnahmen müssen beispielsweise geeignet sein,

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren,
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können,
- zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich im Rahmen ihrer Zugriffsberechtigung zugreifen können und personenbezogene Daten bei der Verarbeitung, Nutzung oder nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- zu gewährleisten, dass zu unterschiedlich Zwecken erhobene Daten getrennt verarbeitet werden können.

Bei den technischen und organisatorischen Maßnahmen ist von entscheidender Bedeutung, dass sie als ein zusammenwirkendes Schutzsystem verstanden werden.

Viele Maßnahmen des Datenschutzes wirken zugleich im Sinne einer Sicherung eines ordentlichen Betriebsablaufs. Deshalb ist es wichtig, das Datenschutzkonzept jeweils in engem Zusam-

menhang mit sonstigen Sicherheitskonzepten zu entwickeln und anzuwenden.

Automatisierte Abrufverfahren gem. § 7 KDO

Während die KDO allgemein im Bezug auf technische Fragen eher zurückhaltend ist, stellt sie für die Einrichtung eines automatisierten Verfahrens zum Abruf personenbezogener Daten durch Dritte gem. § 7 KDO genaue Anforderungen auf, weil sie darin eine besonders einschneidende Maßnahme sieht.

Damit die Zulässigkeit des Abrufverfahrens kontrolliert werden kann, müssen die beteiligten Stellen folgendes schriftlich festlegen:

- Anlass und Zweck des Abrufverfahrens,
- Dritte, an die übermittelt wird,
- Art der zu übermittelnden Daten,
- nach § 6 KDO erforderliche technische und organisatorische Maßnahmen.

Die Einrichtung des automatisierten Abrufverfahrens ist zulässig, wenn es unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen einerseits und der Aufgaben oder Geschäftszwecke der beteiligten Stellen andererseits angemessen ist.

Schließlich ist der Diözesandatenschutzbeauftragte unter Mitteilung der Festlegungen des § 7 Absatz 2 KDO über die Einrichtung von Abrufverfahren zu informieren (§ 7 Absatz 3 KDO).

2.9 Der Beauftragte für den Datenschutz

Gesetzesbestimmungen: §§ 16 ff., 18a ff. KDO

Der Diözesandatenschutzbeauftragte gem. § 16 bzw. der zuständige Ordensdatenschutzbeauftragte sind die „höchste fachliche Instanz“ für Beschwerden in Angelegenheiten des Datenschutzes. Er wacht über die Einhaltung der Bestimmungen dieser Anordnung sowie anderer Vorschriften über den Datenschutz. Er berät die Leitung und die Einrichtungen und kann Empfehlungen zur Verbesserung des Datenschutzes geben. Ferner hat er auf Anforderung Gutachten zu erstellen und Berichte zu verfassen.

Alle drei Jahre hat er der Leitung einen Tätigkeitsbericht zu erstatten.

Dabei soll auch eine Darstellung der wesentlichen Entwicklung des Datenschutzes im nichtkirchlichen Bereich gegeben werden.

Er wirkt auch auf die Zusammenarbeit der übrigen kirchlichen Datenschutzbeauftragten hin und steht auch dem betrieblichen Datenschutzbeauftragten als Ansprechpartner zur Verfügung.

Bei Feststellung von Verstößen gegen die Vorschriften der KDO oder gegen andere Datenschutzbestimmungen oder bei Feststellung sonstiger Mängel bei der Verarbeitung personenbezogener Daten kann er diese gegenüber der zuständigen aufsichtsführenden Stelle beanstanden und diese zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auffordern. Er kann auch von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt. Mit der Beanstandung kann der Diözesandatenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zu sonstigen Verbesserungen des Datenschutzes verbinden. Die zuständige aufsichtsführende Stelle hat bei ihrer Stellungnahme auch eine Darstellung der Maßnahmen

vorzunehmen, die aufgrund der Beanstandung des Diözesandatenschutzbeauftragten getroffen worden sind.

Er wirkt auch auf die Zusammenarbeit der kirchlichen Datenschutzbeauftragten hin und steht auch dem betrieblichen Datenschutzbeauftragten als Ansprechpartner zur Verfügung.

Die **betrieblichen Beauftragten für den Datenschutz gem. § 18 a KDO** sind wichtige Ansprechpartner vor Ort in Fragen des Datenschutzes für die Betroffenen sowie die Beschäftigten in den Behörden und Einrichtungen der Kirche.

In § 18a KDO ist niedergelegt, dass die kirchlichen Stellen einen betrieblichen Datenschutzbeauftragten bestellen können.

Je nach Struktur der Stelle genügt die Bestellung eines Beauftragten auch für mehrere Bereiche.

In § 18a Abs. 2 ist ausdrücklich sogar vorgesehen, dass mit der Aufgabe auch eine Person außerhalb der kirchlichen Stelle beauftragt werden kann und sogar ein betrieblicher Datenschutzbeauftragter auch von mehreren kirchlichen Stellen bestellt werden kann.

Die freiwillige Bestellung eines Datenschutzbeauftragten ist also immer möglich. Sie ist nicht zwingend vorgesehen.
Dies hat aber unter Umständen zur Folge, dass eine Meldepflicht nach § 3a KDO an den Diözesandatenschutzbeauftragten entfällt (§ 3a Abs. 3 KDO).
Der betriebliche Beauftragte für den Datenschutz hat nach dem Gesetz eine herausgehobene Stellung, die sich darin zeigt, dass er dem Leiter der kirchlichen Stelle unmittelbar zu unterstellen ist.

Um seine Unabhängigkeit in der Wahrnehmung seiner fachlichen Aufgaben zu gewährleisten, bestimmt die KDO, dass er in der Ausübung seiner Fachkunde weisungsfrei ist. Damit kann ihm niemand, auch nicht der Leiter der Stelle, vorschreiben, wie er datenschutzrechtliche Fragen bewertet.

Der Leiter der Stelle kann sich aber über das Votum des betrieblichen Datenschutzbeauftragten hinwegsetzen, denn letztlich trägt er die Verantwortung für die Daten verarbeitende Stelle.

Um der hohen Bedeutung des Datenschutzbeauftragten für einen wirkungsvollen Datenschutz Rechnung zu tragen, darf nach der KDO für diese Aufgabe nur bestellt werden, wer die erforderliche „Fachkunde und Zuverlässigkeit“ besitzt. Der fachkundige Datenschutzbeauftragte muss also sowohl die technische als auch die rechtliche Seite seiner Aufgaben kennen und gute Kenntnis in allen Bereichen haben, die für die Organisation, in der er arbeitet, von Bedeutung sind. Nur so hat er die notwendigen Voraussetzungen, dem Datenschutz in seiner Organisation Geltung zu verleihen.

Besonders bedeutsam für alle, die sich mit einer datenschutzrechtlichen Beschwerde oder Frage an ihn wenden, ist die gesetzliche Verschwiegenheitspflicht des Datenschutzbeauftragten (§ 18a Abs. 5 in Verbindung mit § 17 Abs. 4 und 5 KDO).

Über die Identität des Betroffenen (Beschwerdeführers) oder Umstände, die Rückschlüsse hierüber erlauben, darf er keine Auskünfte geben. Eine Ausnahme gilt nur, wenn die betroffene Person ihn von seiner Verschwiegenheitsverpflichtung befreit.

Die Aufgaben des Datenschutzbeauftragten sind vielfältig, insbesondere muss er

- auf die Einhaltung der KDO und anderer Vorschriften über den Datenschutz hinwirken,
- die ordnungsgemäße Programmanwendung überwachen,
- die bei der Verarbeitung personenbezogener Daten eingesetzten Beschäftigten mit den Anforderungen des Datenschutzes vertraut machen,
- die öffentlich zugänglichen Angaben des Verzeichnisses nach § 3a KDO in geeigneter Weise auf Antrag jedermann verfügbar machen. Einer besonderen Berechtigung oder Begründung bedarf es für denjenigen, der von diesem Recht Gebrauch machen möchte, nicht.
- Und er soll mit dem Diözesan- beziehungsweise dem Ordensdatenschutzbeauftragten zusammenarbeiten.

Die (zugeordneten) kirchlichen Stellen müssen dem Datenschutzbeauftragten eine Übersicht über die in § 3a KDO genannten Angaben sowie zugriffsberechtigte Personen zur Verfügung stellen.

Sie sind auch im Übrigen verpflichtet, ihn insgesamt bei der Erfüllung seiner Aufgaben zu unterstützen.
Nach § 3a Abs. 3 entfällt die Meldepflicht, wenn für die verantwortliche Stelle ein betrieblicher Datenschutzbeauftragter nach § 18a bestellt wurde oder bei ihr höchstens zehn Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind.

Zum Schutz des Datenschutzbeauftragten, auch mit dem Ziel der Absicherung seiner Unabhängigkeit, bestimmt die KDO, dass er nicht wegen Erfüllung seiner Aufgaben benachteiligt werden darf (§ 18a, Abs. 3, Satz 2 KDO). Seine Bestellung kann nur unter erschwerten Bedingungen widerrufen werden.

2.10 Zusammenfassung von 2.

Zusammenfassend lassen sich folgende wesentlichen Änderungen durch die neue KDO feststellen:

- Der Anwendungsbereich der KDO wird dahingehend erweitert, dass jegliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus automatisierter Verarbeitung oder in oder aus nicht automatisierten Dateien erfasst wird.
- Bereits bei der Datenerhebung ebenso wie für alle weiteren Phasen der Datenverarbeitung gilt der Zweckbindungsgrundsatz; Ausnahmen sind gesetzlich geregelt.
- Die Datenerhebung wird unter den gesetzlichen Erlaubnisvorbehalt gestellt (gesetzliche Grundlage oder Einwilligung) anstelle der früheren Regel „der Datenerhebung nach Treu und Glauben".
- Der Grundsatz, Daten nur im erforderlichen Umfang zu verarbeiten und Datenvermeidung durch den Einsatz technischer Verfahren zu betreiben ist jetzt gesetzlich festgeschrieben.
- Es wurden Regelungen geschaffen zur Übermittlung personenbezogener Daten auch in das Ausland.
- Es wurde eine einheitliche Rechtsgrundlage für den betrieblichen Beauftragten für den Datenschutz eingeführt, die als Kann-Bestimmung vorgesehen ist.

3. Besonderheiten bei der Datenverarbeitung

3.1 Die Rechte der Betroffenen

Welche Rechte die Betroffenen im Zusammenhang mit der Erhebung, Verarbeitung und Nutzung ihrer Daten haben, regeln insbesondere die §§ 5, 13 und 14 KDO.

Aber auch an anderer Stelle trifft die KDO Regelungen für bestimmte Bereiche, z. B. die Videoüberwachung in § 5a KDO, bei denen sich aus den Pflichten für die Daten verarbeitende Stellen spiegelbildlich die Rechte des Betroffenen ergeben.

3.2 Das Recht auf Auskunft

Gesetzesbestimmung: § 13 KDO

Jeder – unabhängig von Alter, Wohnsitz und Nationalität – hat das Recht auf Auskunft über die zu seiner Person gespeicherten Daten.

3.2.1 Welche Auskunft kann dieser „Jedermann" verlangen?

- Über die zu seiner Person gespeicherten Daten, einschließlich der Angabe, woher sie stammen und an wen sie weitergegeben werden.

Die KDO spricht hier von Empfängern oder Kategorien von Empfängern. Der Begriff des Empfängers umfasst nicht nur Dritte außerhalb der verantwortlichen Stelle, sondern auch natürliche Personen oder Stellen, die im Geltungsbereich der KDO für einen anderen im Auftrag Daten verarbeitende sowie auch verschiedene Organisationseinheiten innerhalb einer Stelle.

Auch die Informationen über die Kategorien der Empfänger können für den Einzelnen von erheblicher Bedeutung sein, z. B. macht es einen Unterschied, ob es sich bei den Empfängern um natürliche Personen handelt oder bestimmte Branchen oder Unternehmen auch in der Kirche, wie z. B. Verlage oder andere geschäftsmäßige Datenverarbeiter usw.

Ferner kann Auskunft verlangt werden über den Zweck der Speicherung (d. h. die betreffende Verwaltungsaufgabe oder einen speziellen Geschäftszweck).

3.2.2 Wie erhält der Betroffene Auskunft

- Es empfiehlt sich, die Auskunft schriftlich anzufordern. Zur Legitimation genügt in der Regel, die Kopie eines Personaldokuments beizulegen. Einschreiben ist nicht erforderlich.
- Bei persönlicher Vorsprache wird eine sofortige Erledigung oft nicht möglich sein.
- Wenn der Betroffene anruft, kann man ihn meist nicht sicher identifizieren. Deshalb gilt hier der **Grundsatz: Keine telefonische Datenauskunft**.
- Der Betroffene sollte möglichst genau beschreiben, worüber er Auskunft wünscht (also z. B. „meine Daten im Zusammenhang mit einem Mietvertrag in x-Stadt“ nicht aber „alles was der Orden über mich hat“).
  Der Betroffene muss sich an die verantwortliche Stelle wenden.
  Außerdem können den Betroffenen die Datenschutzbeauftragten weiterhelfen.

3.2.3 Was kostet eine Auskunft?

Grundsätzlich braucht der Betroffene für die Auskunft nicht zu bezahlen (§ 13 Abs. 6 KDO).

Insgesamt muss der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse stehen. Eine Auskunftserteilung unterbleibt auch, wenn die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen

Stelle liegenden Aufgabe gefährden würde oder die Auskunft dem kirchlichen Wohl Nachteile bereiten würde.

Was kann der Betroffene tun, wenn die Auskunft verweigert wird?
Der Betroffene kann sich an den zuständigen Datenschutzbeauftragten wenden (§ 13 Abs. 5 KDO).

3.3 Einsichtsrecht in das Verfahrensverzeichnis

Die in § 1 Abs. 2 KDO genannten Stellen sind verpflichtet Verfahren automatisierter Verarbeitung vor Inbetriebnahme dem Diözesandatenschutzbeauftragten oder dem Ordensdatenschutzbeauftragten zu melden. Allerdings entfällt die Meldepflicht, wenn für die verantwortliche Stelle ein betrieblicher Datenschutzbeauftragter (§ 18) bestellt wurde oder bei der Stelle höchstens 10 Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind. Dieses Verzeichnis kann von jedermann eingesehen werden, der ein berechtigtes Interesse nachweist (§ 3a Abs. 4 KDO).

Es ist Aufgabe des Datenschutzbeauftragten, auf Antrag die Angaben in dem Verfahrensverzeichnis den Antragstellern/Betroffenen in geeigneter Weise verfügbar zu machen.

Der Inhalt des Verzeichnisses kann dem Betroffenen Anhaltspunkte geben, bezogen auf welche Daten er sein Auskunftsrecht ausüben möchte.
Bis auf die allgemeine Beschreibung, die es ermöglicht, die Maßnahmen zur Gewährleistung der Sicherheit der Bearbeitung zu beurteilen, sind alle Angaben öffentlich.

Hier ist ein wichtiger Hinweis notwendig:

Dem Verzeichnis, wie es in § 3a Abs. 2 niedergelegt ist, kann und darf nicht entnommen werden, ob überhaupt und wenn ja, welche Daten gerade über den Betroffenen oder eine andere Person wo gespeichert sind. Es geht nur um die Zweckbestimmung der Datenerhebung, Verarbeitung oder Nutzung, eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Datenkategorien. Näheres ist in § 3a Abs. 2 KDO geregelt.

Nicht einsehbar sind im Übrigen Verzeichnisse, die einer besonderen Schutzbestimmung (wie die Geheimakten im Diözesanarchiv) unterliegen. Spezielle Regelungen gehen immer vor!

3.4 Die Rechte auf Benachrichtigung, Berichtigung, Sperrung oder Löschung

3.4.1 Die Benachrichtigung

Gesetzesbestimmung: § 13a KDO

Ein anderes wichtiges Mittel, damit der Betroffene wissen kann, wer welche Daten über ihn verarbeitet, ist die Benachrichtigung.
Jede verantwortliche Stelle ist verpflichtet, alle Betroffenen individuell zu benachrichtigen, über die sie Daten ohne deren Kenntnis erhoben hat oder deren Daten sie speichern oder verarbeiten möchte.

Der Zeitpunkt der Benachrichtigung ist unterschiedlich.

Sie hat spätestens bei der ersten Übermittlung zu erfolgen.

Die Benachrichtigung muss umfassen:

- Angabe der verantwortlichen Stelle (z. B. Name und Anschrift),
- die Tatsache, dass erstmals Daten über die Person, die benachrichtigt wird, gespeichert oder übermittelt werden, und die Art der Daten,
- die Zweckbestimmung der Erhebung bei Verarbeitung oder Nutzung,
- sowie die Empfänger oder Kategorien von Empfängern, soweit der Betroffene nicht mit der Übermittlung dieser rechnen muss.

Ausnahmen:
In bestimmten Fällen erfolgt keine Benachrichtigung, etwa weil der Betroffene auf andere Weise von der Speicherung oder der Übermittlung Kenntnis erlangt hat oder die Unterrichtung einen unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Übermittlung durch eine Rechtsvorschrift ausdrücklich vorgesehen ist (§ 13a Abs. 2 KDO).

Eine Benachrichtigung erfolgt darüber hinaus auch nicht, wenn die Voraussetzungen des § 13 Abs. 2 oder 3 KDO vorliegen.

Vorschlag für Angaben auf dem Briefkopf einer speichernden kirchlichen Stelle:

„Hinweis gemäß § 13a KDO: Wir speichern Ihre personenbezogenen Daten."

3.4.2 Das Recht auf Berichtigung

Gesetzesbestimmung: § 14 KDO

Wann sind personenbezogene Daten zu berichtigen?

Jede Stelle ist verpflichtet, unrichtige Daten zu berichtigen. Es liegt aber auch am Betroffenen selbst, darauf hinzuweisen, wenn Daten unrichtig oder überholt sind.

In nicht dateimäßig strukturierten Akten werden unrichtige Daten nicht durch richtige ausgetauscht, es wird aber ein Berichtigungsvermerk beigefügt. Ebenso ist zu vermerken, wenn der Betroffene die Richtigkeit bestreitet.

3.4.3 Wann sind personenbezogene Daten zu löschen?

Die personenbezogenen Daten sind zu löschen, wenn die Speicherung unzulässig ist, weil schon die Erhebung unzulässig war, da

- es sich um Daten über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung oder Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt oder
- ihre Richtigkeit von den verantwortlichen Stellen nicht bewiesen werden kann, oder
- für eigene Zwecke verarbeitete Daten für die Erfüllung des Speicherzwecks nicht mehr erforderlich sind, oder
- geschäftsmäßig zum Zweck der Übermittlung verarbeitete Daten aufgrund einer am Ende des 4. Kalenderjahres nach der ersten Speicherung vorzunehmenden Prüfung nicht mehr erforderlich sind (Adressverlage).

Eine Löschung ist nur für personenbezogene Daten vorgesehen, die entweder aus automatisierter Datenverarbeitung stammen oder aus einer manuellen Datei, jedoch nicht für einzelne Daten, die in nicht dateimäßig strukturierten Akten festgehalten sind.

Sind allerdings komplette Akten unzulässig angelegt, so sind sie ebenfalls zu vernichten.

Ebenso ist im Allgemeinen mit nicht mehr erforderlichen Akten zu verfahren. Dabei ist aber auch die kirchliche Archivordnung zu beachten!

3.4.4 Wann sind personenbezogene Daten zu sperren?

Personenbezogene Daten sind immer dann zu sperren, wenn einer fälligen Löschung besondere Gründe entgegenstehen, etwa

- gesetzlich, satzungsmäßig oder vertraglich festgelegte Aufbewahrungsfristen,
- schutzwürdige Interessen des Betroffenen, etwa weil ihm Beweismittel verloren gingen, oder
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

Personenbezogene Daten, die automatisiert verarbeitet und in nicht automatisierten Dateien gespeichert sind, sind zu sperren, wenn der Betroffene ihre Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn dies

- zu wissenschaftlichen Zwecken,
- zur Behebung einer bestehenden Beweisnot oder
- aus sonstigen, in überwiegendem Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist.

3.5 Das Widerspruchsrecht

Gesetzesbestimmung: § 14 Abs. 5 KDO

Das Widerspruchsrecht nach § 14 Abs. 5 KDO richtet sich gegen die rechtmäßige Datenverarbeitung.

Der Widerspruch ist begründet,

- sofern besondere Umstände in der Person des Betroffenen liegen, und
- das schutzwürdige Interesse des Betroffenen das Interesse der verantwortlichen Stelle an der Erhebung, Verarbeitung oder Nutzung der entsprechenden personenbezogenen Daten überwiegt.

Es gibt kein Widerspruchrecht, wenn eine Rechtsvorschrift eine Verpflichtung zur Erhebung, Verarbeitung oder Nutzung vorschreibt.

3.6 Die Rechte beim Einsatz von Videoüberwachung

Gesetzesbestimmung: § 5a KDO

§ 5a KDO bestimmt die Voraussetzungen, unter denen die „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“ (Videoüberwachung) unlässig ist. Unter „öffentlich zugänglichem Raum“ ist der Raum zu verstehen, in dem sich jedermann berechtigt aufhalten kann, ohne in irgendwelche Rechtsbeziehungen zum Inhaber des Hausrechtes dieses Raumes treten zu müssen. Im Einzelfall bedarf es der Auslegung, was darunter zu fassen ist. Beispiele für öffentlich zugängliche Räume sind nicht nur Kirchen, Museen und sonstige Ausstellungs- und Andachtsräume, sondern auch bestimmte Bereiche von Krankenhäusern und anderen kirchlichen Gebäuden.

Nicht erfasst ist die Beobachtung im Arbeitnehmerbereich innerhalb von kirchlichen Betrieben oder Behörden.

Erlaubt ist die Überwachung zur Aufgabenerfüllung kirchlicher Stellen oder zur Wahrnehmung des Hausrechtes oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke, soweit sie erforderlich ist.
Das bedeutet, dass immer zu prüfen ist, ob es für den angestrebten Zweck wirklich einer Videoüberwachung bedarf, welche Alternativen es hierzu möglicherweise gibt, und ob nicht in das Persönlichkeitsrecht weniger einschneidende Maßnahmen in Frage kommen.

Es muss also eine Erforderlichkeitsprüfung erfolgen. Ferner ist eine Güterabwägung erforderlich.

Ist danach die Videoüberwachung erforderlich, sind weiterhin die mit der Videoüberwachung verfolgten Zwecke gegen die schutzwürdigen Interessen der von der Überwachung Betroffenen abzuwägen. Ergeben sich hier Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen, ist die Videoüberwachung ebenfalls unzulässig.

Keine heimliche Beobachtung!

Eine heimliche Beobachtung ist unzulässig. Die Videoüberwachung muss durch geeignete Maßnahmen kenntlich gemacht werden. Da bei einer Videoüberwachung öffentlich zugänglicher Räume damit gerechnet werden muss, dass Menschen verschiedener Nationalitäten erfasst werden, sollten die Hinweisschilder unter Umständen mehrsprachig sein.

Die hier zu stellenden Anforderungen müssen nach der Lage im Einzelfall beurteilt werden.

Wenn nicht nur eine Beobachtung erfolgen soll, sondern auch eine Verarbeitung oder Nutzung (Speicherung der Filme/Auswertung), sind weitere Zulässigkeitsfragen zu beachten. So hat eine erneute Prüfung der Erforderlichkeit für die weitere Verarbeitung oder Nutzung zu erfolgen. Die Kontrollfrage lautet: **Genügt nicht die einfache Beobachtung?**
Auch eine neue Abwägung mit den schutzwürdigen Interessen des Betroffenen ist durchzuführen.

Wenn die durch Videoüberwachung erhobenen Daten einer bestimmten Person zugeordnet werden, muss diese Person über die Verarbeitung oder Nutzung entsprechend § 13a KDO benachrichtigt werden. So ist gewährleistet, dass diese von der Überwachung und der anschließenden Auswertung Kenntnis erhält und selbst für die Wahrung ihrer Rechte eintreten kann. Daten, die nicht mehr für den angestrebten Zweck der Überwachung benötigt werden, müssen unverzüglich gelöscht werden.

Dasselbe gilt, wenn schutzwürdige Interessen des Betroffenen der weiteren Speicherung entgegenstehen.

3.7 Die Rechte beim Einsatz von Chipkarten

Gesetzesbestimmung: § 5b KDO

§ 5b KDO stellt Regeln für den Einsatz „mobiler personenbezogener Speicher- und Verarbeitungsmedien“ auf. Unter diese Begriffsbestimmung fallen auch die Chipkarten.

Erfasst sind nur Karten mit einem Prozessorchip, z. B. die Karten im Bereich des Gesundheitswesens aber auch zum Betreten von Gebäuden.

Die Stelle, die z. B. Chipkarten ausgibt oder sonst in der in § 5b KDO genannten Art einsetzt, muss den Betroffenen informieren:

1. über ihre Identität und Anschrift
2. über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten in allgemein verständlicher Form,
3. darüber, wie der Betroffene seine Rechte auf Auskunft, Berichtigung, Löschung und Sperrung, sowie das Widerspruchsrecht ausüben kann, und
4. welche Maßnahmen bei Verlust oder Zerstörung der Karte zu treffen sind.

Die Unterrichtungspflicht besteht nicht, wenn der Betroffene bereits auf andere Weise Kenntnis erlangt hat.

Damit das Auskunftsrecht in der Praxis auch wahrgenommen werden kann, müssen in angemessenem Umfang Geräte oder Einrichtungen zur Wahrnehmung des Auskunftsrechts (z. B. Lesegeräte) zur Verfügung gestellt werden.

Auch hier muss die Auskunft unentgeltlich erfolgen.

Weiterhin bestimmt die KDO, dass für den Betroffenen eindeutig erkennbar sein muss, wenn ein Kommunikationsvorgang – beispielsweise den Lesevorgang bei kontaktlosen Chipkarten – auf dem Speichermedium eine Datenverarbeitung auslöst. Er wird so davor geschützt, dass andere ohne seine Kenntnisnahme Daten lesen, eingeben oder sonst verarbeiten.

3.8 Das Recht auf Anrufung des Beauftragten für den Datenschutz

Gesetzesbestimmung: § 15 KDO

Wer annimmt, bei der Erhebung, Verarbeitung oder Nutzung seiner persönlichen Daten durch kirchliche Stellen in seinen Rechten verletzt worden zu sein, kann sich an den Beauftragten für den Datenschutz wenden. Ansprechpartner ist grundsätzlich der Diözesandatenschutzbeauftragte oder der Ordensdatenschutzbeauftragte; aber auch der betriebliche Datenschutzbeauftragte kann von einem Beschwerdeführer angesprochen werden.

Als unabhängige Beschwerdeinstanz mit umfassenden Kontrollbefugnissen geht der Beauftragte Eingaben nach und unterrichtet den Betroffenen vom Ergebnis.

Alle Eingaben werden vertraulich behandelt. Auf Wunsch des Betroffenen bleibt der Name auch gegenüber der Stelle unbenannt, über die er sich beschwert.

3.9 Schadensersatzansprüche des Betroffenen?

Wenn eine verantwortliche Stelle einem Betroffenen durch eine unzulässige oder unrichtige Datenverarbeitung einen Schaden zufügt, ist sie zum Ersatz des Schadens verpflichtet. Zwar gibt es keine ausdrückliche Bestimmung in der KDO zu diesem Fragenkomplex, wie dies beispielsweise beim Bundesdatenschutzgesetz der Fall ist (§§ 7 und 8 BDSG).
Es gelten allerdings die allgemeinen gesetzlichen Schadensersatzregelungen, z. B. § 823 BGB, wonach derjenige, der die Rechte eines anderen vorsätzlich oder fahrlässig verletzt und diesem dabei einen Schaden zufügt, Ersatz leisten muss.

Dies gilt übrigens auch bei einer schweren Verletzung des Persönlichkeitsrechtes hinsichtlich eines Schmerzensgeldes, wenn dem Betroffenen ein Schaden entstanden ist, der nicht als Vermögensschaden anzusehen ist.

Der Schmerzensgeldanspruch bei verschuldensabhängiger Haftung ergibt sich ebenfalls aus dem Bürgerlichen Gesetzbuch (BGB).

In beiden Fällen ist es allerdings so, dass hier der Nachweis, dass ein Schaden entstanden ist und dass die kirchliche Stelle den Schaden zu vertreten hat, seitens des Betroffenen geführt werden muss. Die KDO hat die Beweislastumkehr des BDSG nicht übernommen, wonach die verantwortliche Stelle den Nachweis erbringen muss, dass sie den Schaden nicht zu vertreten hat.

3.10 Was hat sich geändert?

Wesentliche Änderungen im neuen Recht sind:

- Verbesserungen beim Auskunfts-, Benachrichtigungs- und Widerspruchsrecht,
- gesetzliche Vorgaben zu den Zulässigkeitsvoraussetzungen der Videoüberwachung öffentlich zugänglicher Räume,
- Aufnahme einer Regelung zu „mobilen personenbezogenen Speicher- und Verarbeitungsmedien“, (Chipkarten), die Informationspflichten gegenüber dem Betroffenen begründet und damit zu mehr Transparenz und Rechtssicherheit führen soll.

C. Schlussbemerkung

Wie aus dem Vorstehenden ersichtlich wird, sollen nach dem Willen des Bundesverfassungsgerichts, des (staatlichen) Gesetzgebers und auch der europäischen Union die Privatsphäre und die Herrschaft über die eigenen persönlichen Daten gewahrt werden, gerade in einer vernetzten Welt, in der der Einzelne von vielen Datensammlern „ins Visier" genommen wird.

Die deutschen Bischöfe und die Mitglieder der Ordensverbände haben sich dieser Aufgabe gestellt und eigene, gleichwertige Regelungen geschaffen, die den kirchlichen Besonderheiten Rechnung tragen.

Zum Schutz dieser verfassungsrechtlich geschützten Privatsphäre wollen und sollen die kirchlichen Verantwortlichen mithelfen, geeignete Maßnahmen für den Datenschutz zu ergreifen.

Damit schützen wir aber auch ein Menschenbild, das wir als moderne Christen mitentwickelt und uns zu Eigen gemacht haben.

D. Einzelfragen

Nachfolgend sollen einzelne Fragen angesprochen werden, die in der Vergangenheit immer wieder zu Rückfragen und Auskunftsersuchen geführt haben. Dabei war der Verfasser bemüht die wesentlichen Fragen so zu beantworten, wie dies als Ergebnis der Beratungen in der Kommission für Meldewesen und Datenschutz des Verbandes der Diözesen und aufgrund eigener Überlegungen im Einzelfall beantwortet worden ist. Gleichwohl können die nachfolgenden Einzelpunkte nur Empfehlungscharakter haben. Abweichungen und unterschiedliche Auffassun-

gen und Bewertungen von Diözesandatenschutzbeauftragten oder Bistumsverwaltungen sind durchaus möglich und müssen ggf. auch vor dem Hintergrund unterschiedlicher Sachverhalte beurteilt werden.
Zweifelsfragen sollten daher – wenn möglich – immer mit dem Diözesandatenschutzbeauftragten abgestimmt werden.

1. Veröffentlichungen von kirchlichen Amtshandlungen

Bei der Veröffentlichung von kirchlichen Amtshandlungen, wie Erstkommunion, Firmungen, Trauungen und Taufen in kirchlichen Gemeindeblättern mit Namen und Tag, handelt es sich um die Erfüllung einer kirchlichen Aufgabe, nämlich um die Information der Gemeinde und die Förderung der Gemeinschaft, so dass eine Veröffentlichung im Pfarrblatt oder durch Aushang keiner Einwilligung der Betroffenen bedarf.
Eine schriftliche Einverständniserklärung ist jedoch dann einzuholen, wenn beispielsweise die Überlassung der Namen von Erstkommunikanten an Sparkassen oder Firmen erfolgen soll, wie dies bisweilen geschieht. Hierbei handelt es sich nicht mehr um die Erfüllung eines kirchlichen Auftrages. Dies gilt auch für die Überlassung an nicht kirchliche Publikationsorgane, z. B. die örtliche Zeitung.

Die Einwilligung kann in diesen Fällen zweckmäßigerweise schon bei der Anmeldung zu der betreffenden Amtshandlung eingeholt werden.

Unberührt bleibt auch die Zulässigkeit der Veröffentlichung von Aufgeboten durch Vermeldung oder Aushang.

2. Veröffentlichung von Jubiläen

Häufig werden Jubiläen, z. B. der 75. Geburtstag eines Gemeindemitgliedes oder Ehejubiläen, in kirchlichen Gemeindeblättern oder durch Aushang veröffentlicht.
Bei der Frage, ob es sich hierbei um eine datenschutzrechtlich unbedenkliche Erfüllung eines kirchlichen Auftrages handelt, ist wie folgt zu differenzieren:

Im Falle eines Geburtstages liegt keine kirchliche Amtshandlung vor. Die Feier eines Ehejubiläums, an der die Gemeinde im Gottesdienst teilnehmen soll, fällt dagegen in den Bereich der zulässigen Veröffentlichung.

Die Bekanntgabe von Geburtstagen, insbesondere Jubiläumsdaten, sollte nur mit Einwilligung des Betroffenen veröffentlicht werden.

3. Veröffentlichung von Kirchenaustritten

Die Kommission für Meldewesen und Datenschutz, ebenso wie die Kommission für Staatskirchenrecht des Verbandes der Diözesen Deutschlands, vertreten übereinstimmend die Auffassung, dass es grundsätzlich zulässig sein muss, die Namen der ausgetretenen Gemeindemitglieder seitens des Pfarrers bzw. des Pfarrseelsorgers gegenüber der Gemeinde bekannt zu geben und auch seitens der Gemeinde und der einzelnen Gemeindemitglieder dies von ihrem Pfarrseelsorger zu erfahren[1], damit durch das

[1] Im Ergebnis, ebenso AG Landau vom 21.12.1994, C. 354/94; LG Bonn vom 22.03.1985, KirchE 23, 50; Dieter Lorenz, in: Handbuch des Staatskirchenrechts, Band I, 2. Auflage 1994, S. 740, und Christian Meyer, Bemerkungen zum Kirchenmitgliedschaftsrecht, in ZeKR 27 (1982) S. 234 ff., 237. Nach Axel von Campenhausen in Staatskirchenrecht 1973, Fußn. 471, lässt sich ein Anspruch auf Geheimhaltung des

Gebet der Gemeinde und das missionarische Wirken von Seelsorger und Laien diese zurückfinden können.
Dabei stehen ausschließlich pastorale Gesichtspunkte im Vordergrund.

Auch hat die Kommission für Meldewesen und Datenschutz in ihrer Sitzung vom 20.09.1995 zur allgemeinen Veröffentlichung der Namen von Ausgetretenen im Aushang, der auch Nichtkirchenmitgliedern zugänglich ist, folgendes klargestellt:

Unter pastoralen Gesichtspunkten sei es sicherlich erstrebenswert, ja werde es sogar notwendig sein, den Ausgetretenen dazu zu bewegen, seine Entscheidung zu überdenken und gegebenenfalls rückgängig zu machen. Ob aber das Mittel der Bekanntgabe des Kirchenaustrittes dazu erforderlich sei, das sei eine Frage, die in jedem Einzelfall geprüft werden müsse. Es genüge nicht die Zweckmäßigkeit, es genüge auch nicht eine gewisse Erfolgsaussicht, gefordert sei die Notwendigkeit der Datenübermittlung. Ein Mittel, das nicht geeignet sei, den pastoralen Zweck überhaupt zu erfüllen, sei auch nicht erforderlich.

Von kirchlichen Datenschutzbeauftragten wird dagegen die Auffassung vertreten, dass die Veröffentlichung grundsätzlich unzulässig und die Mitteilung an einzelne Personen nur ausnahmsweise zulässig ist, wenn nach sorgfältiger Prüfung auch unter Berücksichtigung schutzwürdiger Interessen des Betroffenen eine Chance besteht, dass die betreffende Einzelperson den

---

Kirchenaustrittes nicht aus Art. 140 GG i.V.m. 136 III WRV ableiten, denn es handele sich nicht um die Offenbarung religiöser Überzeugungen. Ebenso Engelhard, Der Austritt aus der Kirche, S. 79 und Herbert Claessen, Datenschutz in der evangelischen Kirche, 3. Auflage, S. 34 und 35.

Betroffenen zurückgewinnen oder insoweit wenigstens hilfreich sein könnte (vgl. c. 528 § 1 CIC)[2].

Dagegen wird von anderen, insbesondere auch der Rechtsprechung, weiter differenziert[3]. Danach werden keine rechtlichen Bedenken gegen die öffentliche Bekanntmachung des Namens des Ausgetretenen geäußert, weil zwischen der religiösen Überzeugung, die ein sensibles Datum sei, und der rechtlichen Zugehörigkeit zu einer Religionsgemeinschaft – die kein sensibles Datum sei – unterschieden werden müsse. Die Frage der Zulässigkeit der Veröffentlichung der Namen von Ausgetretenen wird daher offenbar weiter zu diskutieren sein.

Deshalb wird folgendes empfohlen:

Neben der rechtlichen Zulässigkeit sollte gleichwohl immer auch nach der pastoralen Zweckmäßigkeit gefragt werden. Dieses Kriterium steht weiter in der Verantwortung des jeweils zuständigen Seelsorgers, der im Einzelfall zu prüfen und zu entscheiden hat, ob eine namentliche Veröffentlichung von Kirchenaustritten gegenüber den Gemeindemitgliedern vorgenommen werden soll, denn eine Veröffentlichung kann auch die Folge haben, dass der Ausgetretene gerade durch diesen Vorgang endgültig der Kirche verloren geht.

---

2 Amtsblatt Augsburg vom 14.01.1999, S. 48.

3 Claessen, a.a.O.; Gaertner, in: Deutsche Tagespost vom 22.09.1995 und Fußnote 1.

4. Weitergabe von Daten an ehrenamtliche Gemeindehelfer/Besucherkreis

Eine Weitergabe von Daten durch den Ortspfarrer an Gemeindehelfer, die beispielsweise neu zugezogene oder ältere Gemeindemitglieder besuchen, ist als Erfüllung eines kirchlichen Auftrages dann unbedenklich, wenn es sich um Daten handelt, die sie für ihre Arbeit benötigen, und wenn die Betreffenden über ihre Verschwiegenheitspflicht belehrt wurden und eine Datenschutzverpflichtung i. S. des § 4 Satz 2 KDO unterschrieben haben.

Gleiches gilt auch für Sammlungen, die von einer kirchlichen (katholischen) Stelle für kirchliche, einschließlich karitativer Zwecke, durchgeführt werden. Auch für diese Gemeindehelfer wird in der Regel lediglich die Weitergabe des Namens und der Adresse zulässig sein, weil weitere Daten für ihre Arbeit nicht erforderlich sind.

5. Weitergabe von Daten an Kirchenzeitungen

Hier ist zunächst zu prüfen, ob es sich tatsächlich um eine Zeitung der Kirche handelt. Ist dies der Fall und kommt der jeweilige Pfarrer zu dem Ergebnis, dass er aus pastoralen Gründen diese Zeitschrift fördern möchte, dann muss auf jeden Fall der Werber auf die Einhaltung des Datenschutzes durch das zuständige Pfarramt verpflichtet werden (s. oben 4.). Zur Werbung für eine kirchliche Zeitung wird in der Regel nur die Bekanntgabe des Namens und der Anschrift von Gemeindemitgliedern erforderlich sein. Die Datenüberlassung ist zur Erfüllung eines kirchlichen Auftrages des Empfängers erforderlich.

Es ist davon auszugehen, dass die Kirchenzeitung (Bistumsblatt) eine kirchliche Aufgabe wahrnimmt, und dass sie in

Wahrnehmung dieser Aufgabe auch Abonnenten werben muss. Eine sinnvolle, d. h. gezielte Werbung, kann ohne entsprechendes Adressenmaterial nicht durchgeführt werden. Dabei hat sich auch die Kirchenzeitung den Vorschriften des § 11 Abs. 3 KDO zu unterwerfen.[4]

Bei überregionalen Zeitungen, die von sich behaupten, der Kirche nahe zu stehen, ist zu differenzieren. Soweit hier keine derartig klar erkennbare, auch rechtlich abgesicherte Zuordnung zu einer kirchlichen Stelle vorliegt, wie es bei den Bistumsblättern der Fall ist, ist Zurückhaltung geboten. Hier empfiehlt es sich, über den Diözesandatenschutzbeauftragten eine Klärung herbeizuführen. Dieser wird dann feststellen, ob die Voraussetzungen für die Kirchlichkeit dieses Publikationsorgans gegeben sind. Entscheidend sind auch hier der Verkündigungsauftrag und die Nähe zur Kirche.

6. Weitergabe von Namen und Adressen von katholischen Patienten an Krankenhauspfarrer

In einer Reihe von Bistümern gibt es bereits bereichsspezifische Datenschutzbestimmungen für katholische Krankenhäuser. Dort wird im Einzelnen geregelt, dass die Weitergabe von Namen und Adressen an den Krankenhausseelsorger zulässig ist. Die Namen und Anschriften der Patienten werden benötigt, damit der Krankenhauspfarrer seine seelsorgerischen Aufgaben erfüllen kann.
Eine besondere schriftliche Einwilligung ist hier nicht erforderlich, da man davon ausgehen kann, dass der Patient mit der Angabe seiner Konfession – welchen Zweck sollte er sonst verfol-

---

4 Für das Bistum Limburg: Feststellung des Generalvikars zur Bistumszeitung vom 06. Juli 1988, Amtsblatt 1988, S. 91 und 92.

gen – auch mit der Überlassung an seinen zuständigen Krankenhausseelsorger einverstanden ist (konkludente Einwilligung).

Dabei wird den Krankenhausverwaltungen zwar das Recht zugestanden, den Patienten nach seiner Konfession zu fragen, dieser ist aber nicht verpflichtet, diese Frage zu beantworten[5].

Zweifelhaft ist, ob eine derartige konkludente Einwilligung auch für eine Datenweitergabe an den Gemeindepfarrer (Heimatpfarrer) und an den ehrenamtlichen Besuchsdienst der Kirchengemeinde angenommen werden kann. Hier könnte der Patient – wenn auch wohl nur in Ausnahmefällen – durchaus entgegenstehende Gründe haben. Die bereichsspezifischen Datenschutzbestimmungen der Bistümer sehen daher für kirchliche Krankenhäuser eine so genannte Widerspruchslösung vor[6]. Diese besagt, dass der Patient einer Weitergabe seiner Daten (nur Name, Adresse und Krankenhausstation) an den Heimatseelsorger widersprechen kann. Sofern keine Regelung dieser Art besteht, sollte auf jeden Fall die Einwilligung durch einen entsprechenden Hinweis bei der Aufnahme eingeholt werden.

Abschließend sei noch einmal nachdrücklich empfohlen, in Zweifelsfragen Rat und Auskunft beim zuständigen Datenschutzbeauftragten des jeweiligen (Erz-) Bistums einzuholen, der in der Regel mit den auftretenden Fragen bereits vertraut ist und wertvolle Ratschläge zur Einhaltung des Datenschutzes und

---

5 Im Ergebnis so auch K. Albrecht, Anstaltsseelsorge, in: Handbuch des Staatskirchenrechts, Band II, Berlin 1975, 715; dort auch bei Problematik des § 203 StGB.

6 Für das Bistum Limburg: Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Rehabilitationskliniken in der Diözese Limburg – PatDSO, Amtsblatt 2006, S. 297 und 311.

Beachtung der Vorschriften der KDO und anderer kirchlicher Datenschutzbestimmungen leistet.

7. Auskunft über Namen und Wohnorte von Verstorbenen

Hier gilt die Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche, die von der Deutschen Bischofskonferenz am 19. September 1988 beschlossen und den Diözesanbischöfen als Diözesangesetz empfohlen wurde.[7]

Dabei sind Sperrfristen zu beachten. Einzelne Aktengruppen und Aktenstücke können von der Benutzung durch Dritte ausgenommen werden. Auch ist eine Verlängerung der Sperrfrist aus wichtigem Grunde möglich. Insbesondere wenn das Wohl der Kirche, schutzwürdige Belange Dritter oder Interessen Betroffener gefährdet oder Persönlichkeitsrechte, Regelungen des staatlichen oder kirchlichen Datenschutzes oder das Steuergeheimnis verletzt würden.

Anträge sind an den Leiter des jeweiligen Diözesanarchivs zu richten, der dann eine interne Klärung vornimmt und auch den Antrag bescheidet.

---

7 Für das Bistum Limburg: Amtsblatt 1988, S. 101 und 102.

5. Muster einer „Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft“

i.d.F. des Beschlusses der Vollversammlung
des Verbandes der Diözesen Deutschlands
vom 25.11.2003

„In der freien Jugendhilfe in kirchlicher Trägerschaft sind für die erhobenen, verarbeiteten und genutzten Sozialdaten das Sozialgeheimnis und dessen Sozialdatenschutzvorschriften (Sozialgesetzbuch I § 35 Abs. 1, Abs. 3 und 4, VIII §§ 62–68, X §§ 67–80, §§ 83 und 84) entsprechend anzuwenden. Im Übrigen gilt die Anordnung zum kirchlichen Datenschutz (KDO).“

6. Merkblatt zum Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft*)

Merkblatt zum Sozialdatenschutz in der freien Jugendhilfe; die Katholische Kirche betreffend
(Neufassung – Stand: Juli 2006)

I. Der Schutz von Sozialdaten und Sozialgeheimnis wird gewährleistet

a) durch die Anordnung des Diözesanbischofs über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft. Diese lautet:

b) „In der freien Jugendhilfe in kirchlicher Trägerschaft sind für die erhobenen, verarbeiteten und genutzten Sozialdaten das Sozialgeheimnis und dessen Sozialdatenschutzvorschriften (Sozialgesetzbuch I § 35 Abs. 1, Abs. 3 und 4, VIII §§ 62–68, X §§ 67–80, §§ 83 und 84) entsprechend anzuwenden. Im Übrigen gilt die Anordnung zum kirchlichen Datenschutz (KDO)."

c) Zusätzlich gelten die **beruflichen Geheimhaltungspflichten**, welche gemäß § 203 StGB geschützt sind (z. B. die Geheimhaltungspflicht der Ehe-, Familien-, Erziehungs- oder Jugendberater in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist sowie der staatlich anerkannten Sozialarbeiter oder Sozialpädagogen).

---

* Gilt uneingeschränkt nur in den (Erz-)Diözesen, die die „Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft" in Kraft gesetzt haben.

Die Sozialdatenschutzvorschriften des Sozialgesetzbuches gelten nicht unmittelbar für den kirchlichen Bereich. Da aber gemäß § 61 Abs. 3 des Sozialgesetzbuches SGB VIII die Träger der freien Jugendhilfe aufgerufen sind, den Schutz von Sozialdaten bei ihrer Erhebung, Verarbeitung oder Nutzung in entsprechender Weise zu gewährleisten, wurde die obige Anordnung des Diözesanbischofs erlassen.

Diese Anordnung verlangt die Beachtung fast aller einschlägigen Sozialdatenschutzvorschriften (mit Ausnahme der speziellen Schadensersatzbestimmungen gemäß § 82 SGB X in Verbindung mit §§ 7 und 8 des Bundesdatenschutzgesetzes. Diesbezüglich gelten die allgemeinen Vorschriften des Bürgerlichen Gesetzbuches; anstatt § 81 SGB X „Rechte des Einzelnen, Datenschutzbeauftragte“ gelten die entsprechenden Vorschriften der KDO).

II. **Sozialdaten** in der freien Jugendhilfe sind demnach alle Daten, die über junge Menschen und deren Familien bekannt werden (z. B. Familienverhältnisse, Vermögensverhältnisse, Gesundheitszustand).

Das **Sozialgeheimnis** gibt jedermann einen Anspruch, dass seine Sozialdaten auch von den Trägern der freien Jugendhilfe und ihren Stellen nicht unbefugt erhoben, verarbeitet oder genutzt werden. Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an Befugte weitergegeben werden. Soweit eine Übermittlung nicht zulässig ist, besteht keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Auslieferung von Unterlagen. Hier stecken die für die öffentlichen Stellen gem. § 35 SGB I geltenden Vorschriften den Rahmen ab. **Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich.**

Die in der Anordnung genannten Vorschriften regeln den Sozialdatenschutz umfassend und ins Einzelne gehend, in weiten

Teilen im Ergebnis nicht anders als die KDO (und das Bundesdatenschutzgesetz):

1. Prinzip der **Datenvermeidung und der Datensparsamkeit** (vgl. auch § 2a KDO): Es dürfen nur Daten erhoben und verwendet werden, welche zur Erfüllung der Aufgaben benötigt werden.

2. Prinzip der **informationellen Selbstbestimmung**: Mit **Einwilligung** eines einwilligungsfähigen Betroffenen und seines gesetzlichen Vertreters (bei fehlender Einwilligungsfähigkeit mit der Einwilligung des gesetzlichen Vertreters allein) dürfen in diesem Rahmen immer Daten erhoben und verwendet werden.

   § 67b Abs. 2 SGB X lautet:

   > Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Die Einwilligung und der Hinweis bedürfen der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

   Die Einwilligung und die Hinweise sind also in der Regel schriftlich (mit Unterschrift) zu erteilen.

   Die Einwilligung kann in der Regel von vorneherein für bestimmte Fälle erteilt werden, z. B. in einem Kindergartenvertrag. Dabei ist die Einwilligungserklärung im äußeren Schriftbild hervorzuheben, vgl. § 67b Abs. 2 SGB X.

3. **Ohne Einwilligung** ist eine Datenerhebung, -verarbeitung und -nutzung nur zulässig, wenn es dafür eine gesetzliche

Ermächtigung gibt. In diesem Fall ist der Grundsatz der **Transparenz** zu beachten, d. h. der Betroffene soll wissen, wer seine Daten und wozu er sie verwendet.

4. Die **Übermittlung** von Sozialdaten an Dritte (vor allem an öffentliche Stellen) ist nur zulässig

a) mit wirksamer Einwilligung,

b) für die Erfüllung des Zwecks, für welchen die Daten befugt erhoben wurden,

c) für die Erfüllung gesetzlicher Aufgaben nach dem Sozialgesetzbuch,

d) soweit das Sozialgesetzbuch die Datenübermittlung ausdrücklich erlaubt und eine Mitteilungspflicht besteht (z. B. nach dem Infektionsschutzgesetz),

e) aus übergeordneten Gesichtspunkten (rechtfertigender Notstand, mutmaßliche Einwilligung bei „Gefahr im Verzug“, Wahrung berechtigter Eigeninteressen in Beweisnot).

5. Von ganz besonderer Bedeutung ist der **besondere Vertrauensschutz in der persönlichen und erzieherischen Hilfe** gemäß § 65 SGB VIII:

Sozialdaten, die dem Mitarbeiter des Trägers der freien Jugendhilfe zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesem nur weitergegeben werden

1. mit der Einwilligung dessen, der die Daten anvertraut hat, oder

2. dem Vormundschafts- oder dem Familiengericht zur Erfüllung der Aufgaben nach § 8 a Abs. 3 SGB VIII,

wenn angesichts einer Gefährdung des Wohls eines Kindes oder eines Jugendlichen ohne diese Mitteilung eine für die Gewährung von Leistungen notwendige gerichtliche Entscheidung nicht ermöglicht werden könnte, oder

3. wenn gewichtige Anhaltspunkte für die Gefährdung des Wohles eines Kindes oder eines Jugendlichen bekannt werden, an die gemäß § 8a Abs. 2 SGB VIII hinzuzuziehende „erfahrene Fachkraft“. Gehört diese nicht der verantwortlichen Stelle an, sind die Daten zu anonymisieren oder pseudonymisieren, soweit die Aufgabenerfüllung dies zulässt oder
4. unter der Voraussetzung, unter denen eine der in § 203 Abs. 1 oder 3 des Strafgesetzbuches genannten Personen dazu befugt wäre (z. B. Notstand).

Gibt der Mitarbeiter anvertraute Sozialdaten weiter, so dürfen sie vom **Empfänger** nur zu dem Zweck weitergegeben werden, zu dem er diese befugt erhalten hat.

Das bedeutet:

a) Ohne Einwilligung dürfen derartige Daten grundsätzlich auch nicht an Vorgesetzte und andere Mitarbeiter weitergegeben werden;

b) ohne Einwilligung dürfen Aufzeichnungen über derartige Daten anderen nicht überlassen werden. Solche Aufzeichnungen sind grundsätzlich zu vernichten, sobald sie nicht mehr benötigt werden.

zu a) und b):

Deshalb kann es zweckmäßig sein, z. B. beim Abschluss eines Kindergartenvertrages, entsprechende Einwilligungen einzufordern.

6. Erstreckung des Sozialgeheimnisses auf die (befugten) Empfänger von Sozialdaten:

a) Hinsichtlich des besonderen Vertrauensschutzes in der persönlichen und erzieherischen Hilfe.

b) Hinsichtlich der von einem Arzt oder einem anderen Berufsgeheimnisträger gem. § 203 Abs. 1 und Abs. 3 StGB mitgeteilten Daten.

c) Wenn kirchliche Einrichtungen von staatlichen Stellen Sozialdaten empfangen, dürfen sie diese nur zu dem Zweck verarbeiten oder nutzen, zu denen sie ihnen befugt übermittelt worden sind.

Vgl. dazu § 65 Abs. 1 S. 2 SGB VIII, § 76 Abs. 1 SGB X und § 78 SGB X.

7. Zur Übermittlung von Sozialdaten an Dritte, insbesondere staatliche Stellen, im Einzelnen:

Diese Übermittlung ist enger und strenger geregelt als durch die allgemeinen Datenschutzbestimmungen.

a) Besonders eng ist der oben beschriebene besondere Vertrauensschutz in der persönlichen und erzieherischen Hilfe gemäß § 65 SGB VIII; es wird die Auffassung vertreten, dass diesbezüglich sogar die Rechnungsprüfungsämter keine Einsicht in derartige Auf-

zeichnungen nehmen dürfen (vgl. hinsichtlich der übrigen Aufzeichnungen § 69 Abs. 5 SGB X).

b) Übermittlungsbefugnisse nach dem SGB sind vor allem geregelt in § 64 SGB VIII sowie den §§ 67 bis 75 SGB X.
Von diesen Bestimmungen dürften in der Praxis die §§ 64 SGB VIII sowie die §§ 69, 71 Abs. 1 Nr. 1 und 2, § 75 SGB X in Betracht kommen.

Die Bestimmungen finden Sie z. B. im Internet unter www.sozialgesetzbuch-bundessozialhilfegesetz.de

Soweit diese Bestimmungen nur die Befugnis zur Datenübermittlung regeln (vgl. oben 4 d), ist zu prüfen, ob eine Verpflichtung des freien Trägers dazu besteht. Diese kann auch außerhalb des SGB normiert sein. Besteht keine Verpflichtung, sollte von einer Datenübermittlung abgesehen werden.

Zu § 69-**Datenübermittlung zur Erfüllung sozialer Aufgaben** sowie der gesetzlichen **Aufgaben** der **Rechnungshöfe** und anderer Kontrollorgane:

Falls die Datenübermittlung befugt nicht zu dem Zweck geschieht, zu welchem die Daten erhoben wurden (Zweckdurchbrechung) darf der Erfolg der zu gewährenden Leistung nicht infrage gestellt werden (§ 64 Abs. II SGB VIII).

Zu § 71-**Übermittlung für die Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse**:

Zulässig ist demnach (selbstverständlich) die Erfüllung der gesetzlichen Mitteilungspflichten zur Abwendung geplanter besonders schwerer Straftaten gemäß

§ 138 StGB sowie zum Schutz der öffentlichen Gesundheit nach § 8 des Infektionsschutzgesetzes vom 20. Juli 2000.
Anfragen der Ausländerbehörden sollten ohne Einwilligung nicht beantwortet werden, da freie Träger und deren Einrichtungen nicht die vom Gesetz vorausgesetzte Auskunftspflicht haben.

Zu § 75-**Übermittlung von Sozialdaten für die Forschung und Planung**:
Eine Datenübermittlung zu Planungszwecken öffentlicher Stellen kommt in aller Regel nur mit Einwilligung der Betroffenen in Betracht (vgl. § 75 Abs. 1 Satz 2).

Soweit für eine Datenübermittlung (ohne Einwilligung) die Genehmigung der zuständigen „obersten Bundes- oder Landesbehörde“ vorgeschrieben ist, führt die angeordnete „entsprechende“ Anwendung der Vorschrift zum Erfordernis der Genehmigung des Diözesanbischofs (vgl. auch die kirchliche Archivordnung; kommt in der Praxis für wissenschaftliche Forschung in Betracht).

Bemerkenswert ist noch:

Die in § 68 und § 73 SBG X angesprochene Datenübermittlung an Behörden, welche für die öffentliche Sicherheit und Ordnung zuständig sind sowie für die Durchführung eines Strafverfahrens richtet sich an **öffentliche Stellen**, welche zur **Amtshilfe** verpflichtet sind. Träger der freien Jugendhilfe und deren Einrichtungen dürften nicht gemeint sein.

Jedoch können diese Vorschriften von Bedeutung für den Umfang einer entsprechenden Anwendung von § 35 Abs. 3 SGB I z. B. für die Frage der Zeugnisverweigerung sein.

III. In Zweifelsfällen, vor allem soweit noch keine Erfahrungen vorliegen, wird dringend empfohlen, beim Diözesandatenschutzbeauftragten oder, soweit ein betrieblicher Datenschutzbeauftragter bestellt wurde, zunächst bei diesem, nachzufragen. Nicht vergessen werden sollte, dass Datenschutz auch die Sicherung der Daten vor unbefugten Dritten sowie vor unbeabsichtigter Vernichtung bedeutet und dass diesbezüglich angemessene Maßnahmen zu treffen sind.

Datenschutzbeauftragter der bayerischen (Erz-)Diözesen im Juli 2006

7. Anordnung über das kirchliche Meldewesen (Kirchenmeldewesenanordnung – KMAO)

i.d.F. des Beschlusses der Vollversammlung
des Verbandes der Diözesen Deutschlands
vom 20./21.06.2005

Die staatlichen oder kommunalen Meldebehörden (Meldebehörden) übermitteln der Katholischen Kirche in ihrer Eigenschaft als öffentlich-rechtliche Religionsgesellschaft zur Erfüllung ihrer Aufgaben nach Maßgabe der Meldegesetze Daten (Meldedaten). Empfänger der Daten sind die Bistümer und/oder für ihren Bereich die Kirchengemeinden/Pfarreien.

In diesem Zusammenhang wird folgendes angeordnet:

§ 1
Mitgliedschaft

(1) Als Mitglied der katholischen Kirche im Sinne dieser Anordnung (Kirchenmitglied) gilt jeder, der durch die Taufe in der katholischen Kirche oder durch Übertritt von einer anderen Kirche oder christlichen Religionsgemeinschaft oder durch Wiederaufnahme der katholischen Kirche angehört und nicht nach den Bestimmungen des staatlichen Rechts aus der Kirche ausgetreten ist.

(2) Die Kirchenmitgliedschaft wird vermutet, wenn die Daten des staatlichen oder kommunalen Melderegisters entsprechende Angaben enthalten.

§ 2
Datenschutz und andere Bestimmungen

(1) Die Anordnung über den kirchlichen Datenschutz (KDO) in der jeweils geltenden Fassung sowie bereichsspezifische Regelungen sind zu beachten.

(2) Die kirchenrechtlichen Regelungen zur Führung der Kirchenbücher werden durch diese Anordnung nicht berührt.

§ 3
Mitwirkungspflichten der Kirchenmitglieder

(1) Die Kirchenmitglieder sind verpflichtet, sich bei der zuständigen Meldebehörde bei der Gründung eines neuen oder eines weiteren Wohnsitzes anzumelden.

(2) Die Kirchenmitglieder sind verpflichtet, bei den Meldebehörden ihre Bekenntniszugehörigkeit anzugeben.

(3) Das Bistum und die Kirchengemeinde/Pfarrei sind berechtigt, Daten (Meldedaten und kirchliche Daten) von dem Kirchenmitglied unmittelbar anzufordern; das Kirchenmitglied ist verpflichtet, die Daten mitzuteilen. Durch bischöfliche Anordnung kann festgelegt werden, dass das Kirchenmitglied auch verpflichtet ist, sich bei der zuständigen kirchlichen Stelle anzumelden.

§ 4
Zusammenarbeit mit den Meldebehörden

(1) Die zuständigen kirchlichen Stellen, insbesondere die Kirchengemeinden/Pfarreien sind verpflichtet, gespendete Taufen, Wiederaufnahmen und Übertritte zur Katholischen Kirche den Meldebehörden mitzuteilen.

(2) Ist in den Melderegistern der Meldebehörden die Angabe über die Bekenntniszugehörigkeit von Kirchenmitgliedern falsch oder fehlt sie ganz, so haben die zuständigen kirchlichen Stellen die Berichtigung oder Ergänzung zu veranlassen.

(3) Wird festgestellt, dass ein Kirchenmitglied seiner staatlichen Meldepflicht ganz oder teilweise nicht nachgekommen ist, so ist dieses aufzufordern, die veranlasste Meldung nachzuholen. Auf etwaige ordnungsrechtliche Folgen ist hinzuweisen.

(4) Werden von der Meldebehörde Daten eines nachweislich verstorbenen Kirchenmitglieds übermittelt, soll die Meldebehörde vom Tod des Kirchenmitglieds verständigt werden.

§ 5
Gemeindemitgliederverzeichnis

(1) Zur Führung eines Gemeindemitgliederverzeichnisses sind das Bistum und die Kirchengemeinde/Pfarrei befugt. Die Kirchengemeinde/Pfarrei ist dazu verpflichtet.

(2) Das Gemeindemitgliederverzeichnis kann im Weg der elektronischen Datenverarbeitung geführt werden. Dies kann auch von zentralen kirchlichen Rechenzentren besorgt werden.

(3) Das Gemeindemitgliederverzeichnis enthält die für die Erfüllung des kirchlichen Auftrags erforderlichen Meldedaten. Es enthält ferner kirchliche Daten, die sich aus den Kirchenbüchern (Matrikeln) ergeben, insbesondere Daten über Taufe, Erstkommunion, Firmung, Trauung, Weihe und Profess sowie über Aufnahme und Wiederaufnahme von Kirchenmitgliedern.

(4) Diese Daten werden zwischen den Stellen, welche das Gemeindemitgliederverzeichnis führen, ausgetauscht.

(5) Auskunfts- und Übermittlungssperren müssen ihrem Zweck entsprechend beachtet werden.

(6) Das Bistum kann die Daten aller Gemeindemitgliederverzeichnisse in seinem Bereich erheben, verarbeiten oder nutzen.

Die Kirchengemeinde/Pfarrei kann nur die Daten des Gemeindemitgliederverzeichnisses ihres Bereichs erheben, verarbeiten oder nutzen.

Der Generalvikar regelt die Zugriffsberechtigung für das Gemeindemitgliederverzeichnis des Bistums durch Ausführungsvorschrift nach Maßgabe der Prinzipien der KDO, insbesondere dem Prinzip der Erforderlichkeit und der Datensparsamkeit.

Für den Bereich der Kirchengemeinde/Pfarrei regelt dies der Pfarrer bzw. der verantwortliche Leiter.

§ 6
Inkrafttreten

Diese Anordnung tritt am ..... in Kraft; zum gleichen Zeitpunkt wird die Anordnung über das kirchliche Meldewesen (Kirchenmeldewesenanordnung – KMAO) vom ….....aufgehoben.

8. Einführung in die Kirchenmeldewesenanordnung

(Winfried Fischer, Landgerichtspräsident a. D., Datenschutzbeauftragter der Bayerischen (Erz-)Diözesen)

Die Kommission für Meldewesen und Datenschutz des Verbandes der Diözesen Deutschlands hat folgende Erläuterung beschlossen:

Die bisher geltende Anordnung über das kirchliche Meldewesen (KMAO) war (in den westdeutschen Diözesen) seit den Jahren 1978 bzw. 1979 in Kraft.

Die seitherige Entwicklung der Technik, z. B. der Einsatz zentraler Server (vgl. dazu § 5 Abs. 2), die Neufassung der Anordnung über den kirchlichen Datenschutz (KDO) sowie der Beitritt der ostdeutschen Diözesen mit Wirkung vom 01. Januar 1991 zum Verband der Diözesen Deutschlands ließen eine Neufassung auch der KMAO wünschenswert erscheinen.

Bewährte Regelungen wurden übernommen (z. B. § 1 – Mitgliedschaft). Die KMAO versteht sich als die dem staatlichen Meldewesen entsprechende kirchliche Regelung.

Die Mitwirkungspflichten der Kirchenmitglieder (§ 3) und die Zusammenarbeit der kirchlichen Stellen mit den Meldebehörden (§ 4) sollen nicht nur der Richtigkeit und Vollständigkeit der Meldedaten dienen, sondern auch zum Ausdruck bringen, dass die von den Meldebehörden übermittelten Daten – auch – kirchliche Daten sind.

Der Datenschutz ist grundsätzlich in der KDO geregelt, wenngleich einzelne Bestimmungen der KMAO datenschutzrechtliche Bezüge aufweisen (vgl. § 2 Abs. 1).

Die Bestimmung über die Aufnahme der in den Kirchenbüchern (Matrikeln) zu dokumentierenden kirchlichen Amtshandlungsdaten (vgl. § 5 Abs. 3 S. 2) ist als programmatische Forderung zu verstehen (soweit die bisher geführten Gemeindemitgliederverzeichnisse diese Daten noch nicht enthalten). Insbesondere wäre wünschenswert, diese Daten bei künftigen kirchlichen Amtshandlungen zu übernehmen.

Schließlich stellen sowohl die Präambel als auch die Regelung über das Gemeindemitgliederverzeichnis (vgl. § 5 Abs. 1, Abs. 4 sowie Abs. 6) klar, dass Herr der Daten – jeweils für seinen/ihren Bereich sowohl das Bistum als auch die Kirchengemeinde/Pfarrei sind.

Es kann angezeigt sein, dass sich Bistum und Kirchengemeinde/Pfarrei gegenseitig vorab informieren, wenn solche Daten Dritten übermittelt werden sollen, wobei selbstverständlich die Übermittlungsvorschriften der KDO zu beachten sind.

Ergänzend wird folgendes bemerkt:

1. Datenschutz (§ 2, auch § 5 Abs. 5 KMAO)

Die Bestimmungen des Melderechtsrahmengesetzes und der Landesmeldegesetze über die Zulässigkeit von Auskünften an den Betroffenen selbst (vgl. § 8 MRRG) und von Melderechtsregisterauskünften an Dritte (vgl. § 21 MRRG) richten sich an die Meldebehörden und nicht an kirchliche Stellen. Für letztere gelten die in der Regel strengeren Bestimmungen der KDO. Soweit jedoch die

Meldegesetze ausnahmsweise strengere Vorschriften enthalten, sind diese zu berücksichtigen.

Damit der kirchliche Datenschutz auf dem Gebiet des Meldewesens in jedem Fall dem Standard des staatlichen Datenschutzes gleich kommt, bestimmt § 5 Abs. 5 KMAO, dass Auskunfts- und Übermittlungssperren ihrem Zweck entsprechend berücksichtigt werden müssen.

a) Das bedeutet für Auskünfte an den Betroffenen selbst, dass übergeordnete öffentliche oder private Interessen entgegenstehen können, dieses wird nur in seltenen Ausnahmefällen vorkommen (vgl. auch § 13 Abs. 3 KDO).
   Im Fall der Daten eines betroffenen Kirchenmitglieds, welches an Kindesstatt angenommen wurde, ist das Adoptionsgeheimnis entsprechend § 61 Abs. 2 des Personenstandsgesetzes sowie § 1758 BGB[8] zu beachten.

---

[8] **§ 61 PStG – [Einsicht]**
(1) [1]Einsicht in die Personenstandsbücher, Durchsicht dieser Bücher und Erteilung von Personenstandsurkunden kann nur von den Behörden im Rahmen ihrer Zuständigkeit und von Personen verlangt werden, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen. [2]Behörden haben den Zweck anzugeben. [3]Andere Personen haben nur dann ein Recht auf Einsicht in die Personenstandsbücher, auf Durchsicht dieser Bücher und auf Erteilung von Personenstandsurkunden, wenn sie ein rechtliches Interesse glaubhaft machen.
(2) [1]Ist ein Kind angenommen, so darf nur Behörden, den Annehmenden, deren Eltern, dem gesetzlichen Vertreter des Kindes und dem über sechzehn Jahre alten Kind selbst Einsicht in den Geburtseintrag gestattet oder eine Personenstandsurkunde aus dem Geburtenbuch erteilt werden. [2]Ist ein angenommenes Kind im Familienbuch der Annehmenden eingetragen, so gilt hinsichtlich des dieses Kind betreffenden Eintrags

für die Einsicht in das Familienbuch sowie für die Erteilung einer Personenstandsurkunde aus dem Familienbuch Satz 1 entsprechend. [3]Diese Beschränkungen entfallen mit dem Tod des Kindes; § 1758 des Bürgerlichen Gesetzbuches bleibt unberührt.
(3) [1]Sind bei einer Person auf Grund des Gesetzes über die Änderung der Vornamen und die Feststellung der Geschlechtszugehörigkeit in besonderen Fällen vom 10. September 1980 (BGBl. I S. 1654) die Vornamen geändert oder ist festgestellt worden, dass diese Person als dem anderen Geschlecht zugehörig anzusehen ist, so darf nur Behörden und der betroffenen Person selbst Einsicht in den Geburtseintrag gestattet oder eine Personenstandsurkunde aus dem Geburtenbuch erteilt werden. [2]Ist die betroffene Person in einem Familienbuch eingetragen, so gilt hinsichtlich des sie betreffenden Eintrags für die Einsichtnahme in das Familienbuch und für die Erteilung einer Personenstandsurkunde aus diesem Familienbuch Satz 1 entsprechend. [3]Diese Beschränkungen entfallen mit dem Tod dieser Person; § 5 Abs. 1 und § 10 Abs. 2 in Verbindung mit § 5 Abs. 1 des Gesetzes über die Änderung der Vornamen und die Feststellung der Geschlechtszugehörigkeit in besonderen Fällen bleiben unberührt.

§ 1758 BGB – Offenbarungs- und Ausforschungsverbot
(1) Tatsachen, die geeignet sind, die Annahme und ihre Umstände aufzudecken, dürfen ohne Zustimmung des Annehmenden und des Kindes nicht offenbart oder ausgeforscht werden, es sei denn, dass besondere Gründe des öffentlichen Interesses dies erfordern.
(2) [1]Absatz 1 gilt sinngemäß, wenn die nach § 1747 erforderliche Einwilligung erteilt ist. [2]Das Vormundschaftsgericht kann anordnen, dass die Wirkungen des Absatzes 1 eintreten, wenn ein Antrag auf Ersetzung der Einwilligung eines Elternteils gestellt worden ist.

§ 1747 - Einwilligung der Eltern des Kindes
(1) Zur Annahme eines Kindes ist die Einwilligung der Eltern erforderlich. Sofern kein anderer Mann nach § 1592 als Vater anzusehen ist, gilt im Sinne des Satzes 1 und des § 1748 Abs. 4 als Vater, wer die Voraussetzung des § 1600 d Abs. 2 Satz 1 glaubhaft macht.
(2) Die Einwilligung kann erst erteilt werden, wenn das Kind acht Wochen alt ist. Sie ist auch dann wirksam, wenn der Einwilligende die schon feststehenden Annehmenden nicht kennt.

b) Bei Auskünften an **Dritte** ist eine mitgeteilte Sperre wegen Gefahr für Leben, Gesundheit, persönliche Freiheit oder andere schutzwürdige Interessen für den Betroffenen oder eine andere Person zu beachten. Ferner sind das Adoptionsgeheimnis gemäß § 1758 BGB und dementsprechend § 61 Abs. 2 des Personenstandsgesetzes sowie § 61 Abs. 3 des Personenstands-

---

(3) Sind die Eltern nicht miteinander verheiratet und haben sie keine Sorgeerklärungen abgegeben,

1. kann die Einwilligung des Vaters bereits vor der Geburt erteilt werden,
2. darf, wenn der Vater die Übertragung der Sorge nach § 1672 Abs. 1 beantragt hat, eine Annahme erst ausgesprochen werden, nachdem über den Antrag des Vaters entschieden worden ist,
3. kann der Vater darauf verzichten, die Übertragung der Sorge nach § 1672 Abs. 1 zu beantragen. Die Verzichtserklärung muss öffentlich beurkundet werden. § 1750 gilt sinngemäß mit Ausnahme von Absatz 4 Satz 1.

(4) Die Einwilligung eines Elternteils ist nicht erforderlich, wenn er zur Abgabe einer Erklärung dauernd außerstande oder sein Aufenthalt dauernd unbekannt ist.

§ 1750 – Erklärung der Einwilligung

(1) [1]Die Einwilligung nach §§ 1746, 1747 und 1749 ist dem Vormundschaftsgericht gegenüber zu erklären. [2]Die Erklärung bedarf der notariellen Beurkundung. [3]Die Einwilligung wird in dem Zeitpunkt wirksam, in dem sie dem Vormundschaftsgericht zugeht.

(2) [1]Die Einwilligung kann nicht unter einer Bedingung oder einer Zeitbestimmung erteilt werden. [2]Sie ist unwiderruflich; die Vorschrift des § 1746 Abs. 2 bleibt unberührt.

(3) [1]Die Einwilligung kann nicht durch einen Vertreter erteilt werden. [2]Ist der Einwilligende in der Geschäftsfähigkeit beschränkt, so bedarf seine Einwilligung nicht der Zustimmung seines gesetzlichen Vertreters. [3]Die Vorschrift des § 1746 Abs. 1 Satz 2, 3 bleibt unberührt.

(4) [1]Die Einwilligung verliert ihre Kraft, wenn der Antrag zurückgenommen oder die Annahme versagt wird. [2]Die Einwilligung eines Elternteils verliert ferner ihre Kraft, wenn das Kind nicht innerhalb von drei Jahren seit dem Wirksamwerden der Einwilligung angenommen wird.

gesetzes im Hinblick auf das Gesetz über die Änderung der Vornamen und die Feststellung der Geschlechtszugehörigkeit in besonderen Fällen vom 10. September 1980 („Transsexuellengesetz“[9] – BGBl. I S. 1654) als Auskunftssperren zu berücksichtigen. Soweit Ausnahmen für Auskünfte an Behörden vorgesehen sind, gelten diese für die Bistümer und Kirchengemeinden/Pfarreien entsprechend. Diese Datenempfänger müssen die Auskunfts- und Übermittlungssperren entsprechend beachten.

2. Mitwirkungspflichten der Kirchenmitglieder (§ 3 KMAO)

Die Anmeldepflicht gemäß § 3 Abs. 1 ist kirchlicher Natur. Sie entspricht der staatsbürgerlichen Meldepflicht. Minderjährige werden hinsichtlich ihrer Mitwirkungspflichten von ihren gesetzlichen Vertretern vertreten (vgl. can. 97 und 98 CIC).

3. Zusammenarbeit mit den Meldebehörden (hier: § 4 Abs. 3 Satz 2 KMAO)

Mit den ordnungsrechtlichen Folgen, auf die hingewiesen werden soll, sind die Sanktionen gemeint, welche in den Meldegesetzen vorgesehen sind, insbesondere hinsichtlich der Vernachlässigung der An- und Abmeldepflicht.

9 Text abgedruckt unter http://bundesrecht.juris.de/tsg/.

4. Vorabinformation für den Fall einer Datenübermittlung an Dritte – letzter Satz der Einführung –

Gemeint sind Fälle, bei denen Anhaltspunkte dafür bestehen, dass der Dritte z. B. ein gemeinnütziger Verein sowohl an das Bistum als auch an eine Kirchengemeinde/ Pfarrei mit der Bitte um Datenübermittlung herangetreten ist, z. B. zum Zweck einer Spendensammlung. Die Vorabinformation soll voneinander abweichende Entscheidungen verhindern.

9. Fundstellen datenschutzrechtlicher und melderechtlicher Vorschriften in kirchlichen Amtsblättern

Anordnung über den kirchlichen Datenschutz (KDO)

(Erz-)Bistum	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Aachen	21.08.2003	01.10.2003	230	01.10.2003
Augsburg	16.09.2003	23.09.2003	437	01.11.2003
Bamberg	10.10.2003	24.10.2003	360	01.11.2003
Berlin	20.08.2003	01.10.2003	100	01.10.2003
Dresden-Meißen	25.11.2004	06.12.2004	216	01.01.2005
Eichstätt	09.12.2003	09.12.2003	229	01.01.2004
Erfurt	10.12.2003	11.12.2003	53	01.01.2004
Essen	11.09.2003	24.10.2003	98	01.10.2003
Freiburg	30.12.2003	16.01.2004	224	01.01.2004
Fulda	26.01.2004	03.03.2004	29	03.03.2004
Görlitz	o. D.	29.08.2003	1	01.09.2003
Hamburg	31.10.2003	15.11.2003	149	01.11.2003
Hildesheim	15.10.2003	31.10.2003	215	01.11.2003
Köln	26.09.2003	14.10.2003	249	26.09.2003
Limburg	25.09.2003	15.11.2003	203	01.01.2004
Magdeburg	o. D.	10.01.2005	13	01.02.2005
Mainz	12.12.2003	13.01.2004	31	01.01.2004
München und Freising	29.09.2003	15.10.2003	302	01.12.2003
Münster (nrw Teil)		15.10.2003	220	
Münster (oldenbg. Teil)	19.11.2003	15.12.2003	285	01.12.2003
Osnabrück		07.11.2003	306	
Paderborn		26.09.2003	168	
Passau		01.10.2003	1[10]	01.11.2003
Regensburg		30.10.2003	137	01.01.2004
Rottenburg-Stuttgart		13.10.2003	629	
Speyer	17.11.2003	14.01.2004	2	01.01.2004
Trier		01.11.2003	248	
Würzburg		25.10.2003	281	01.11.2003

[10] Sonderausgabe

Durchführungsverordnung zur KDO (KDO-DVO)

(Erz-)Bistum	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Aachen	04.09.2003	01.10.2003	243	01.10.2003
Augsburg	o. D.	23.09.2003	459	01.09.2003
Bamberg	o. D.	24.10.2003	384	01.09.2003
Berlin	03.09.2003	01.10.2003	107	01.10.2003
Dresden-Meißen	26.11.2004	06.12.2004	229	01.01.2005
Eichstätt	09.12.2004	09.12.2003	246	01.01.2004
Erfurt	o. D.	11.12.2003	62	01.01.2004
Essen	11.09.2003	24.10.2003	107	01.10.2003
Freiburg	o. D.	16.01.2004	234	01.01.2004
Fulda	26.01.2004	03.03.2004	36	03.03.2004
Görlitz	o. D.	29.08.2003	16	01.09.2003
Hamburg	o. D.	15.11.2003	158	01.11.2003
Hildesheim	15.10.2003	31.10.2003	233	01.11.2003
Köln	o. D.	14.10.2003	257	[11]
Limburg	25.09.2003	15.11.2003	212	01.01.2004
Magdeburg	o.D.	10.01.2005	13	01.02.2005
Mainz	15.12.2003	13.01.2004	31	01.01.2004
München und Freising		15.10.2003	324	
Münster (nrw Teil)		15.10.2003	229	
Münster (oldenbg. Teil)	19.11.2003	15.12.2003	294	19.11.2003
Osnabrück		07.11.2003	315	
Paderborn		26.09.2003	176	
Passau		01.10.2003	12[12]	
Regensburg		30.10.2003	146	
Rottenburg-Stuttgart		13.10.2003	638	
Speyer	19.11.2003	14.01.2004	23	01.01.2004
Trier		01.11.2003	2	
Würzburg		25.10.2003	297	

[11] Die Inkraftsetzung erfolgt mit dem Datum der Veröffentlichung im Amtsblatt.

[12] Sonderausgabe

Anordnung über das kirchliche Meldewesen (Kirchenmeldewesenanordnung- KMAO) - Neufassung 2005 -

(Erz-)Bistümer	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Aachen	14.10.2006	01.11.2005	272	01.01.2006
Augsburg	12.12.2005	12.12.2005	514	01.01.2006
Bamberg	07.10.2005	25.10.2005	434	01.10.2005
Berlin	17.10.2005	01.11.2005	129	01.11.2005
Dresden-Meißen	10.10.2005	10.10.2005	168	01.10.2005
Eichstätt	19.10.2005	19.10.2005	233	19.10.2005
Erfurt				
Essen	21.03.2006	28.04.2006	56	01.04.2006
Freiburg				
Fulda	09.01.2006	09.01.2006	1	01.12.2005
Görlitz	16.09.2005	19.09.2005	16	01.10.2005
Hamburg	31.10.2005	15.11.2005	207	01.01.2006
Hildesheim	01.11.2005	14.11.2005	290	01.01.2006
Köln	24.10.2005	01.12.2005	347	01.01.2006
Limburg	21.12.2005	15.01.2006	224	01.01.2006
Magdeburg	01.07.2006	01.08.2006	55	01.07.2006
Mainz	14.11.2005	14.12.2005	171	01.01.2006
München	23.09.2005	27.10.2005	507	01.01.2006
Münster (nrw Teil)	01.09.2005	01.10.2005	193	01.10.2005
Münster (oldenb. Teil)	14.10.2005	15.01.2006	43	01.12.2005
Osnabrück	07.10.2005	16.11.2005	295	01.11.2005
Paderborn	26.10.2005	30.11.2005	201	01.01.2006
Passau	01.12.2005	15.12.2005	101	01.01.2006
Regensburg	15.11.2005	15.11.2005	158	01.01.2006
Rottenburg-Stuttgart	15.02.2006	15.03.2006	54	01.04.2006
Speyer	14.12.2005	10.02.2006	12	01.01.2006
Trier	29.11.2005	01.01.2006	12	01.10.2005
Würzburg	24.01.2006	15.03.2006	66	01.03.2006

Weitere bereichsspezifische datenschutzrechtliche Regelungen der (Erz-)Bistümer

(Stand: 01.04.2010)

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Aachen (vollständige Übersicht)				
Personenbezogene Daten im Zusammenhang mit dem Weltjugendtag	o. D.	01.07.2005	163	
Ausführungsbestimmungen zum Datenschutz beim Einsatz von Informationstechnik	05.09.2005	01.10.2005	250	01.10.2005
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Bistum Aachen (PatDSO)	05.09.2005	01.10.2005	246	01.10.2005
Ausführungsrichtlinien zur Anordnung über den Kirchlichen Datenschutz – KDO für den pfarrlichen Bereich	05.09.2005	01.10.2005	249	01.10.2005
Anordnung über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen im Bistum Aachen 1. Änderung	01.08.2006 29.01.2010	01.09.2006 01.03.2010	252 97	01.09.2006 01.02.2010
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	22.07.1991	15.08.1991	114	01.09.1991
Augsburg (Auswahl)				
Übermittlung personenbezogener Daten im Zusammenhang mit dem Weltjugendtag	o. D.	20.04.2005	202	
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe	o. D.	23.09.2003	469	
Veröffentlichung von Kirchenaustritten	o. D.	14.01.1999	48	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	05.10.1988	13.10.1988	709	

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Bamberg (Auswahl)				
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	19.05.2004	28.06.2004	211	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	17.11.1988	30.12.1988	313	
Berlin (Auswahl)				
Datenschutz und Weltjugendtag - Muster einer Verpflichtungserklärung	o. D.	01.05.2005	49	
Datenübermittlung im Zusammenhang mit den Fusionen der Kirchengemeinden	o. D.	01.10.2003	109	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche		01.01.1989	9	
Begründung zur Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche		01.01.1989	11	
Dresden-Meißen (Auswahl)				
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	01.02.1991	10.05.1993	125	
Sicherung und Nutzung von Pfarrmatrikeln (Kirchenbücher)	16.10.2009	23.10.2009	149	
Richtlinien für die Benutzung älterer Kirchenbücher im Bistum Dresden-Meißen	16.10.2009	23.10.2009	150	
Eichstätt (Auswahl)				
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft		11.08.2004	188	

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
(noch Eichstätt)				
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche		11.11.1988	294	
Erfurt (vollständige Übersicht)				
Anordnung über den Sozial datenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft		14.09.2004	54	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	01.04.1993	08.04.1993	Heft 4, S. 2	01.04.1993
Essen (vollständige Übersicht)				
Anordnung über den Sozial-datenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	06.12.2004	21.01.2005	4	
Anordnung über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Träger-schaft im Bistum Essen (KDO-Schulen) 1. Änderung (Anlage 1)	29.12.2005 04.11.2009	27.01.2006 20.11.2009	1 215	01.01.2006 01.12.2009
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Bistum Essen – PatDSO -	29.12.2005	27.01.2006	7	01.01.2006
Ausführungsbestimmungen zum Datenschutz beim Einsatz von Informationstechnik	29.12.2005	27.01.2006	11	01.01.2006
Ausführungsrichtlinien zur Anordnung über den kirchlichen Datenschutz - KDO	29.12.2005	27.01.2006	14	01.01.2006
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	18.11.1988	20.12.1988	147	01.01.1989

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Freiburg (Auswahl)				
Übermittlung personenbezogener Daten im Zusammenhang mit dem Weltjugendtag 2005	o. D.	23.05.2005	76	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	12.12.1988	09.01.1989	6	
Fulda (Auswahl)				
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Rehabilitations-kliniken in der Diözese Fulda (PatDSO)	13.11.2006	06.12.2006	107	01.11.2006
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	15.11.1988	29.12.1988	96	01.01.1989
Görlitz (vollständige Übersicht)				
Anordnung über den Sozialdaten-schutz in der freien Jugendhilfe in kirchlicher Trägerschaft	o. D.	14.01.2004	4	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	12.12.1990	20.02.1991	12	01.01.1990
Pfarrbrief und Datenschutz	29.08.2001	29.08.2001	3	
Veröffentlichung von Kirchenaus-tritten (Datenschutz)	o. D.	30.06.1999	2	
Hamburg (vollständige Übersicht)				
Anordnung über den Sozial-datenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft		15.03.2005	34	
Verpflichtungserklärung für ehrenamt-liche Mitarbeiter in den Kirchen-gemeinden in Zusammenhang mit der Durchführung des Weltjugendtages 2005		01.06.2005	221	

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens

(noch Hamburg)

Die nachfolgenden Vorschriften wurden vom Bistum Osnabrück vor Errichtung des Erzbistums Hamburg erlassen. Sie gelten aufgrund des Konkordatsvertrages auch für die neu gegründete Erzdiözese Hamburg. Sie wurden im Amtsblatt der Erzdiözese Hamburg jedoch nicht neu veröffentlicht. Im Kirchlichen Amtsblatt erschienen lediglich Hinweise, welche Vorschriften weiter gelten. Im einzelnen: Kirchl. Amtsblatt für die Erzdiözese Hamburg vom 15.12.1995, Bd. 1, Nr. 14, Art. 153, S. 140; Kirchl. Amtsblatt für die Erzdiözese Hamburg vom 17.01.1996, Bd. 2 Nr. 1, Art. 14, S. 15

In der nachfolgenden Übersicht ist daher jeweils die Fundstelle im Amtsblatt des Bistums Osnabrück angegeben.

Richtlinien zum Einsatz von Arbeitsplatz-computern in der Diözese Osnabrück	27.07.1994	12.08.1994	68	01.08.1994
Anordnung zum Schutz personen-bezogener Daten in katholischen Schulen in freier Trägerschaft				
in der Diözese Osnabrück	15.06.1989	23.06.1989	200	01.08.1989
1. Änderung	23.07.1991	27.08.1991	249	15.08.1991
Ordnung zum Schutz von Patienten-daten in katholischen Krankenhäusern				
in der Diözese Osnabrück	21.03.1990	30.03.1990	41	01.04.1990
1. Änderung	30.06.1995	16.06.1995	242	01.08.1995
Ordnung zum Schutz von personen-bezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Osnabrück	01.09.1992	25.09.1992	98	01.01.1993
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	15.11.1988	18.11.1988	124	
Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentations-gutes aufgrund von Sondergenehmi-gungen	23.08.1993	08.10.1993	237	
Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte	24.11.1991	26.11.1991	282	

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Hildesheim (vollständige Übersicht)				
Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Hildesheim (KDO-Schulen)	07.03.2008	25.03.2008	72	01.04.2008
Ausführungsvorschrift zu § 7 der Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Hildesheim	07.03.2008	25.03.2008	78	01.04.2008
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	01.08.2004	17.08.2004	235	17.18.2004
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Hildesheim	01.03.1990	22.03.1990	80	01.04.1990
Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft	01.12.1992	21.12.1992	305	01.01.1993
Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche	12.12.1988	22.12.1988	391	12.12.1988
Besonderer Schutz von Computerprogrammen nach dem Urheberrechtsgesetz	01.10.1993	28.01.1994	49	01.10.1993
Datenschutz bei der Übermittlung personenbezogener Daten über Telefax	01.11.1992	23.11.1992	260	01.11.1992
Richtlinien für den Einsatz von Informationstechnik sowie den Datenschutz am Arbeitsplatz in der Diözese Hildesheim	01.07.1991	23.05.1991	126	01.07.1991
Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Hildesheim	01.11.1994	07.12.1994	413	01.11.1994
Veröffentlichung von persönlichen Daten (z.B. Altersjubiläum) in Pfarrbriefen und ähnlichen Publikationen	08.01.1998	23.01.1998	24	08.01.1998

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
(noch Hildesheim)				
Verlängerung der Geltung bereichsspezifischer datenschutzrechtlicher Ausführungsbestimmungen zur Anordnung über den kirchlichen Datenschutz	18.12.2003	16.01.2004	20	18.12.2003
Anordnung zum Schutz personenbezogener Daten bei der Durchführung von Fundraising-Maßnahmen im Bistum Hildesheim – FundrO	15.02.2006	31.03.2006	88	01.01.2006
Sicherung und Nutzung von Pfarrmatrikeln (Kirchenbüchern)	13.02.2008	25.03.2008	70	13.02.2008
Köln (vollständige Übersicht)				
Anordnung über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Trägerschaft im Erzbistum Köln (KDO-Schulen)	02.02.2006	01.03.2006	57	01.03.2006
1. Änderung	22.10.2009	01.11.2009	237	01.11.2009
Ausführungsbestimmungen zum Datenschutz beim Einsatz von Informationstechnik	01.09.2005	01.10.2005	314	01.09.2005
Verpflichtungserklärung für ehrenamtliche Mitarbeiter in den Kirchengemeinden in Zusammenhang mit der Durchführung des Weltjugendtages 2005		01.06.2005	221	
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	14.01.2004	01.03.2004	96	01.03.2004
Ausführungsrichtlinien zur Anordnung über den kirchlichen Datenschutz (AusfRL-KDO)	01.09.2005	01.10.2005	313	01.10.2005
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Erzbistum – PatDSO -	01.09.2005	01.10.2005	304	01.10.2005
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	14.10.1988	01.11.1988	219	

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Limburg (vollständige Übersicht)				
Richtlinie für den Einsatz von Informationstechnik in der Diözese Limburg	21.12.2005	15.01.2006	225	01.01.2006
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Rehabilitationskliniken in der Diözese Limburg – PatDSO 1. Änderung	29.08.2006 13.11.2006	10.10.2006 01.12.2006	297 311	01.11.2006
Ordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Limburg	25.09.2003	15.11.2003	215	01.01.2004
Anordnung zum kirchlichen Datenschutz hinsichtlich der Bekanntmachung besonderer Ereignisse	24.02.1999	15.03.1999	26	
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	14.01.2004	01.03.2004	277	01.03.2004
Übermittlung personenbezogener Daten im Zusammenhang mit dem Weltjugendtag 2005	25.05.2005	10.06.2005	108	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	17.10.1988	01.11.1988	101	01.11.1988
Anordnung über die Sicherung und Nutzung von Pfarrmatrikeln (Kirchenbücher) im Bistum Limburg	10.04.2008	01.06.2008	49	
Magdeburg (Auswahl)				
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	14.07.2006	01.08.2006	56	14.07.2006
Mainz (vollständige Übersicht)				
Ordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Mainz	15.12.1992	20.01.1993	22	01.01.1993

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
(noch Mainz)				
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	o. D.	10.11.2004	236	10.11.2004
„Weltjugendtag 2005“ – Datenschutzrechtlicher Hinweis	o. D.	19.05.2005	64	19.05.2005
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Mainz	29.10.1996	30.10.1996	115	01.11.1996
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	22.11.1988	15.12.1988	123	
München u. Freising (Auswahl)				
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	16.06.2004	28.07.2004	286	
Datenschutzbestimmungen für eine regelmäßige Pflege der Daten von Pfarreien im Internetauftritt des Erzbistums	o. D.	20.12.2006	436	jährlich wiederholend
Suchmaschine für Pfarreien im Internetportal des Erzbistums München und Freising und Angebote von privaten Unternehmen	o. D.	20.12.2006	436	
Datenschutz im Hinblick auf die Übermittlung von Pilgerdaten an ehrenamtliche Mitarbeiter vor Ort in den Kirchengemeinden (Weltjugendtag)	o. D.	30.05.2005	214	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	28.12.1988	13.02.1989	126	
Richtlinien für die Benutzung von Arbeitsplatzcomputern (APC) im Bereich des erzbischöflichen Ordinariats		27.06.2001	245	

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Münster (nrw Teil) (vollständige Übersicht)				
Anordnung über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen im Bistum Münster, nordrheinwestfälischer Teil (KDO-Schulen) 1. Änderung (Anlage 1)	01.09.2005 06.10.2009	01.10.2005 01.11.2009	208 200	01.10.2005 01.11.2009
Ausführungsbestimmungen zur Anordnung über den kirchlichen Datenschutz (KDO) vom 10.01.1979 für die Verarbeitung von personenbezogenen Daten in den kirchlichen freien Schulen des Bistums Münster, nrw Teil	01.11.1989	15.11.1989	186	
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Bistum Münster, nordrheinwestfälischer Teil – PatDSO -	01.09.2005	01.10.2005	205	01.10.2005
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	22.04.2004	15.05.2004	126	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	16.12.1988	01.06.1998	139	
Ausführungsbestimmungen zum Datenschutz beim Einsatz von Informationstechnik	01.09.2005	01.10.2005	215	01.10.2005
Ausführungsrichtlinien zur Anordnung über den kirchlichen Datenschutz – KDO – für den pfarramtlichen Bereich	01.09.2005	01.10.2005	218	01.10.2005
Dienstanweisung über die Benutzung und Behandlung elektronischer Post (E-Mails) im Bischöflichen Generalvikariat und Offizialat Münster[13]	01.03.2004			01.04.2004
Dienstanweisung über die Nutzung des Internets im Bischöflichen Generalvikariat und Offizialat Münster[14]	08.06.2005			01.07.2005

[13] veröffentlicht in: von Cohausen-Schüssler [Hrsg.], Information zum kirchlichen Datenschutz im Bistum Münster, Münster 2006.

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
Münster (oldenburgischer Teil) (Auswahl)				
Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft im Offizialatsbezirk Oldenburg	06.07.1989	15.11.1989	184	01.08.1989
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	21.05.2004	15.06.2004	138	
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern im Offizialatsbezirk Oldenburg	o. D.	01.05.1995	116	
Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft	01.12.1992	15.12.1992	181	01.01.1993
Richtlinien zum Einsatz von Arbeitsplatzcomputern in der röm.-kath. Kirche im oldenburgischen Teil des Bistums Münster	09.08.1994	15.11.1994	152	15.11.1994
Osnabrück (vollständige Übersicht)				
Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Osnabrück (vom 01.09.1989) Neufassung	21.04.2008	19.05.2008	56	01.06.2008
Ausführungsvorschrift zu § 7 der Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Osnabrück	21.04.2008	19.05.2008	59	01.06.2008
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück 1. Änderung	21.03.1990 30.06.1995	30.03.1990 16.06.1995	41 242	01.04.1990 01.08.1995
Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Osnabrück	01.09.1992	25.09.1992	98	01.01.1993

[14] wie Fn. 12.

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
(noch Osnabrück)				
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	15.11.1988	18.11.1988	124	
Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen	23.08.1993	08.10.1993	237	
Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte	24.11.1991	26.11.1991	282	
Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Osnabrück	27.07.1994	12.08.1994	68	01.08.1994
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	12.10.2004	16.11.2004	145	
Weltjugendtag 2005, Datenschutz	08.06.2005	22.06.2005	225	
Paderborn (Auswahl)				
Anordnung über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Trägerschaft im Erzbistum Paderborn (KDO-Schulen)	24.06.1998	30.07.1998	70	01.07.1998
1. Änderung (Anlage 1)	23.10.2009	29.10.2009	116	01.12.2009
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft		28.05.2004	80	
Umgang mit personenbezogenen Daten im Zusammenhang mit dem Weltjugendtag 2005	o. D.	31.05.2005	81	
Ausführungsrichtlinien zur Anordnung über den kirchlichen Datenschutz für das Erzbistum Paderborn	15.07.2005	29.08.2005	133	01.09.2005
Verwaltungsverordnung zum Datenschutz beim Einsatz von Informationstechnik (IT-VVO)	15.07.2005	29.08.2005	133	01.09.2005

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
(noch Paderborn)				
Verordnung zur Bestimmung der zuständigen Stelle im Sinne von § 5 Abs. 3 Satz 1 der Verwaltungsverordnung zum Datenschutz beim Einsatz von Informationstechnik (IT-VVO)	25.08.2006	29.09.2006	113	01.10.2006
Anordnung über die Sicherung und Nutzung der kirchlichen Archive im Erzbistum Paderborn	17.12.2007	28.01.2008	9	28.01.2008
Passau (Auswahl)				
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft		24.05.2004	47	
Übermittlung personenbezogener Daten im Zusammenhang mit dem Weltjugendtag 2005	o. D.	01.06.2005	36	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	19.09.1988	29.11.1988	121	01.12.1998
Regensburg (Auswahl)				
Übermittlung personenbezogener Daten im Zusammenhang mit dem Weltjugendtag 2005	o. D.	09.05.2005	61	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	03.11.1988	10.11.1988	158	01.12.1988
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe		18.12.2002	142	
Rottenburg-Stuttgart (Auswahl)				
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft	04.02.2004	15.03.2004	59	
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche		13.12.1989	735	

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
(noch Rottenburg-Stuttgart)				
Anordnung zum Schutz personenbezogener Daten bei der Durchführung von Fundraising-Maßnahmen im Bistum Rottenburg-Stuttgart	01.12.2006	22.12.2006	309	
Einrichtung des betrieblichen Datenschutzbeauftragten für die Kurie	30.11.2009	15.12.2009	340	
Ausführungsvorschrift zur Anordnung über den kirchlichen Datenschutz zur Gewährleistung des Schutzes personenbezogener Daten bei der Durchführung von Fundraisingmaßnahmen in der Diözese Rottenburg-Stuttgart	02.12.2009	15.12.2009	342	
Speyer (vollständige Übersicht)				
Ordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Speyer	01.04.2004	11.05.2004	122ff	01.04.2004
Schutz personenbezogener Daten im Zusammenhang mit dem Weltjugendtag 2005 - Verpflichtungserklärung	o. D.	14.06.2005	467	
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe	17.11.2003	14.01.2004	22	01.01.2004
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Speyer	o. D.	13.07.1995	456	01.07.1995
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	10.11.1988	25.11.1988	270	01.01.1989
Trier (vollständige Übersicht)				
Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft		01.06.2004	199	
Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Rehabilitationskliniken im Bistum Trier	20.12.2006	01.01.2007	13	01.01.2007

(Erz-)Bistum Sachverhalt	Datum	Amtsblatt vom	Seite	Datum des Inkrafttretens
(noch Trier)				
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	09.11.1988	15.11.1988	263	01.01.1989
Würzburg (Auswahl)				
Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche	01.12.1988	01.12.1988	551	
Anordnung über den Sozialdaten-schutz in der Jugendhilfe in kirchlicher Trägerschaft	05.04.2004	16.04.2004	71	
Sicherung und Nutzung von Kirchenbüchern	o. D.	01.07.2008	222	

10. Datenschutzbeauftragte

(Stand: 13. Februar 2017)
Aktualisierungen erfolgen auf der Website:
http://www.dbk.de/imperial/md/content/schriften/dokumente/datenschutzbeauftragte.pdf

Bistum Aachen
Leiter des Katholischen Datenschutzzentrums
Steffen Pau
Brackeler Hellweg 144
44309 Dortmund
Tel.: 0231/138985-0
Fax: 0231/138985-22
E-Mail: info@kdsz.de

Bistum Augsburg
Vorsitzender Richter am Bayerischen Obersten Landesgericht a. D.
Jupp Joachimski
Rochusstraße 5-7
80333 München
Tel.: 089/21371796
Fax: 089/2137271796
E-Mail: jjoachimski@ordinariat-muenchen.de

Erzbistum Bamberg
Vorsitzender Richter am Bayerischen Obersten Landesgericht a. D.
Jupp Joachimski
Rochusstraße 5-7
80333 München
Tel.: 089/21371796
Fax: 089/2137271796
E-Mail: jjoachimski@ordinariat-muenchen.de

Erzbistum Berlin
Datenschutzbeauftragter der ostdeutschen Bistümer
Matthias Ullrich
Chausseestraße 1
39281 Schönebeck
Tel.: 03928/72 87 181
Fax: 03928/72 87 182
E-Mail: matthias.ullrich@datenschutzbeauftragter-ost.de

Bistum Dresden-Meißen
Datenschutzbeauftragter der ostdeutschen Bistümer
Matthias Ullrich
Chausseestraße 1
39281 Schönebeck
Tel.: 03928/72 87 181
Fax: 03928/72 87 182
E-Mail: matthias.ullrich@datenschutzbeauftragter-ost.de

Bistum Eichstätt
Vorsitzender Richter am Bayerischen Obersten Landesgericht a. D.
Jupp Joachimski
Rochusstraße 5-7
80333 München
Tel.: 089/21371796
Fax: 089/2137271796
E-Mail: jjoachimski@ordinariat-muenchen.de

Bistum Erfurt
Datenschutzbeauftragter der ostdeutschen Bistümer
Matthias Ullrich
Chausseestraße 1
39281 Schönebeck
Tel.: 03928/72 87 181
Fax: 03928/72 87 182
E-Mail: matthias.ullrich@datenschutzbeauftragter-ost.de

Bistum Essen
Leiter des Katholischen Datenschutzzentrums
Steffen Pau
Brackeler Hellweg 144
44309 Dortmund
Tel.: 0231/138985-0
Fax: 0231/138985-22
E-Mail: info@kdsz.de

Erzbistum Freiburg
Michael Keller
Fischerau 6
Tel.: 0761/28537669
Fax: 0761/281029
E-Mail: keller@ddsb-freiburg.de

Bistum Fulda
Rechtsdirektor Rainer Büttner
Paulustor 5
36037 Fulda
Tel.: 0661/87303
Fax: 0661/87304
E-Mail: rechtsabteilung@bistum-fulda.de

Bistum Görlitz
Datenschutzbeauftragter der ostdeutschen Bistümer
Matthias Ullrich
Chausseestraße 1
39281 Schönebeck
Tel.: 03928/72 87 181
Fax: 03928/72 87 182
E-Mail: matthias.ullrich@datenschutzbeauftragter-ost.de

Erzbistum Hamburg
Andreas Mündelein
Schwachhhauser Heerstr. 67
28211 Bremen
Tel.: 0421/16 301925
E-Mail: a.muendelein@datenschutz-katholisch-nord.de

Bistum Hildesheim
Andreas Mündelein
Schwachhhauser Heerstr. 67
28211 Bremen
Tel.: 0421/16 301925
E-Mail: a.muendelein@datenschutz-katholisch-nord.de

Erzbistum Köln
Leiter des Katholischen Datenschutzzentrums
Steffen Pau
Brackeler Hellweg 144
44309 Dortmund
Tel.: 0231/138985-0
Fax: 0231/138985-22
E-Mail: info@kdsz.de

Bistum Limburg
Ann Kristin Waschke
Roßmarkt 4
65549 Limburg
Tel.: 06431/295-159
Fax: 06431/295-387
E-Mail: a.waschke@bistumlimburg.de

Bistum Magdeburg
Datenschutzbeauftragter der ostdeutschen Bistümer
Matthias Ullrich
Chausseestraße 1
39281 Schönebeck
Tel.: 03928/72 87 181
Fax: 03928/72 87 182
E-Mail: matthias.ullrich@datenschutzbeauftragter-ost.de

Bistum Mainz
Oberrechtsrat Günter Zwingert
Bischofsplatz 2
55116 Mainz
Tel.: 06131/253423
Fax: 06131/253556
E-Mail: datenschutz@bistum-mainz.de

Erzbistum München-Freising
Vorsitzender Richter am Bayerischen Obersten Landesgericht a. D.
Jupp Joachimski
Rochusstraße 5-7
80333 München
Tel.: 089/21371796
Fax: 089/2137271796
E-Mail: jjoachimski@ordinariat-muenchen.de

Bistum Münster (NRW-Teil)
Leiter des Katholischen Datenschutzzentrums
Steffen Pau
Brackeler Hellweg 144
44309 Dortmund
Tel.: 0231/138985-0
Fax: 0231/138985-22
E-Mail: info@kdsz.de

Bistum Münster (Oldenburg. Teil)
Andreas Mündelein
Schwachhhauser Heerstr. 67
28211 Bremen
Tel.: 0421/16 301925
E-Mail: a.muendelein@datenschutz-katholisch-nord.de

Bistum Osnabrück
Andreas Mündelein
Schwachhhauser Heerstr. 67
28211 Bremen
Tel.: 0421/16 301925
E-Mail: a.muendelein@datenschutz-katholisch-nord.de

Erzbistum Paderborn
Leiter des Katholischen Datenschutzzentrums
Steffen Pau
Brackeler Hellweg 144
44309 Dortmund
Tel.: 0231/138985-0
Fax: 0231/138985-22
E-Mail: info@kdsz.de

Bistum Passau
Vorsitzender Richter am Bayerischen Obersten Landesgericht a. D.
Jupp Joachimski
Rochusstraße 5-7
80333 München
Tel.: 089/21371796
Fax: 089/2137271796
E-Mail: jjoachimski@ordinariat-muenchen.de

Bistum Regensburg
Vorsitzender Richter am Bayerischen Obersten Landesgericht a. D.
Jupp Joachimski
Rochusstraße 5-7
80333 München
Tel.: 089/21371796
Fax: 089/2137271796
E-Mail: jjoachimski@ordinariat-muenchen.de

Bistum Rottenburg-Stuttgart
N. N.

Bistum Speyer
Rechtsdirektor Hartmut Junkes
Ursulinenstraße 67
66111 Saarbrücken
Tel.: 0681/9068221
Fax: 0681/9068229
E-Mail: kabusa@t-online.de

Bistum Trier
Rechtsdirektor Hartmut Junkes
Ursulinenstraße 67
66111 Saarbrücken
Tel.: 0681/9068221
Fax: 0681/9068229
E-Mail: kabusa@t-online.de

Bistum Würzburg
Vorsitzender Richter am Bayerischen Obersten Landesgericht a. D.
Jupp Joachimski
Rochusstraße 5-7
80333 München
Tel.: 089/21371796
Fax: 089/2137271796
E-Mail: jjoachimski@ordinariat-muenchen.de