

Datenschutz in der Katholischen Kirche

Sicherheit und Ordnungsgemäßheit kirchlicher Datenverarbeitung

Lutz Grammann

Datenschutz in der kirchlichen Erwachsenenbildung

Eine Handreichung

Stand: Juni 2010

Der Diözesandatenschutzbeauftragte
der Erzbistümer Berlin und Hamburg,
der Bistümer Hildesheim, Magdeburg, Osnabrück
und des Bischöflich Münsterschen Offizialats in Vechta i.O.



DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Datenschutz in der kirchlichen Erwachsenenbildung

Der Schutz des Rechts auf informationelle Selbstbestimmung ist selbstverständlich auch im Bereich der Erwachsenenbildung zu gewährleisten. Dabei gilt für Einrichtungen in Trägerschaft der katholischen Kirche die Anordnung über den kirchlichen Datenschutz – KDO – und die zu ihr ergangene Ausführungsvorschrift (KDO-DVO). Die nachfolgenden Ausführungen sollen auf die wesentlichen Aspekte hierbei hinweisen und zum Nachdenken über die eigene Arbeit anregen. Für weitere Fragen steht der Diözesandatenschutzbeauftragte jederzeit zur Verfügung:

Der Diözesandatenschutzbeauftragte
der (Erz-)Bistümer Berlin, Hamburg, Hildesheim, Magdeburg, Osnabrück und des Offizialats Vechta
Engelbosteler Damm 72 • 30167 Hannover • Tel. 0511 – 81 93 15 • Fax 0511 – 81 21 35
E-Mail: info@datenschutz-kirche.de • Internet: <http://www.datenschutz-kirche.de>

I: Datenerhebung

§ 2 Abs. 3 KDO versteht unter „Datenerhebung“ das Beschaffen von Informationen über den Betroffenen. „Betroffener“ ist dabei jede bestimmte oder bestimmbare natürliche Person. Zur Durchführung von Kursen, Seminaren, Tagungen, etc. werden Daten der angemeldeten Teilnehmer benötigt. Zum Schutz ihres Persönlichkeitsrechts ist eine solche Datenerhebung aber nur dann zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat, § 3 Abs. 1 KDO.

Für die Beschaffung von Daten über Kursteilnehmer gelten daher bestimmte Regeln:

- Es dürfen nur die Daten erhoben werden, deren Kenntnis zur Aufgabenerfüllung notwendig sind - § 9 Abs. 1 KDO. Hierzu gehören:
 - Name und Anschrift zur Identifikation des Teilnehmers
 - Kontoverbindungen, soweit sie für Zahlungsvorgänge benötigt werden.
 - Daten über die Voraussetzungen zur Kursteilnahme.
 - Daten über den Arbeitgeber, falls dieser die Kosten der Kursteilnahme trägt.
- Weitere Daten dürfen nur mit Einwilligung des Betroffenen erhoben werden. Dabei ist auf die Freiwilligkeit besonders hinzuweisen. Die Erklärung hat in der Regel schriftlich zu erfolgen - § 3 Abs. 2 KDO
- Die Daten sind beim Betroffenen selbst zu erheben - § 9 Abs. 2 Satz 1 KDO. Dies geschieht in der Regel durch Anmeldeformulare, die vom Betroffenen selbst auszufüllen und zu unterschreiben sind. Werden die Daten auf einer Website im Internet erhoben, sind auch die Anforderungen des Telemediengesetzes zu erfüllen. Hierzu die nachfolgende Tabelle.
- Die Daten dürfen nur für Zwecke gespeichert, verändert oder genutzt werden, für die sie erhoben worden sind - § 10 Abs. 1 KDO.
- Der Betroffene hat jederzeit Anspruch auf unentgeltliche Auskunft über die über ihn erhobenen und gespeicherten Daten und deren Verwendung - § 13 Abs. 1 KDO. Die Form der Auskunftserteilung ist nicht vorgeschrieben. Die Aushändigung eines Ausdrucks des gespeicherten Datensatzes ist jedoch in der Regel zweckmäßig.
- Die Rechtmäßigkeit der Datenerhebung ist unabhängig vom Ort ihrer späteren Speicherung. Für Daten in Akten, Listen, etc. gelten die gleichen Grundsätze, wie für EDV-mäßig erfasste Daten. § 1 Abs. 1 will das Persönlichkeitsrecht des Betroffenen umfassend schützen.

Datenerhebung im Internet

Wer die Anmeldung zu Kursen durch Bereithalten eines entsprechenden Formulars auf seiner Website im Internet ermöglicht, hat zusätzlich zu den oben genannten Grundsätzen auch die Vorschriften des Telemediengesetzes zu beachten. Erforderlich ist in jedem Fall

- ein Impressum nach § 5 TMG und
- eine Datenschutzerklärung (Privacy Policy) nach § 13 TMG

Dabei ist sicherzustellen, dass der Teilnehmer die Datenschutzerklärung gelesen und akzeptiert hat, bevor er auf das elektronische Anmeldeformular weitergeleitet wird. Genaue Hinweise und Muster zur Gestaltung von Impressum und Datenschutzerklärung finden Sie in der Broschüre „Das neue Telemediengesetz (TMG) - Pflichten für kirchliche Internetanbieter bei der Gestaltung von Webseiten“ auf der Homepage „Datenschutz in der katholischen Kirche“.

<http://www.datenschutz-kirche.de/download/tmg-280607.pdf>

Besonders wichtig ist der Zahlungsvorgang. Sollen im Anmeldeformular Angaben zur Kontoverbindung oder Kreditkarte gemacht werden, so muss hierzu auf eine sichere Seite (<https://...>) mit Secure Socket Layer (SSL) weitergeleitet werden.

II. Datenübermittlung/-austausch

Datenübermittlung ist nach § 2 Abs. 4 Nr. 3 KDO das Bekanntgeben personenbezogener Daten an Dritte. Dies können andere Behörden, aber auch Privatpersonen sein. Auch für die Datenübermittlung bedarf es einer Rechtsgrundlage. Ansonsten ist sie nur mit Einwilligung der Betroffenen zulässig.

- Die Übermittlung von Daten an andere kirchliche Stellen, die ebenfalls der KDO unterliegen (§ 1 Abs. 2 KDO), ist nach § 11 Abs. 1 KDO zulässig, wenn sie erforderlich ist,
 - zur Erfüllung, der in der Zuständigkeit der übermittelnden oder empfangenden Stelle liegenden Aufgaben und
 - die Übermittlung dem gleichen Zweck dient, für den die Daten erhoben worden sind.
- Die Übermittlung von Daten an staatliche Stellen ist unter den gleichen Voraussetzungen statthaft, § 11 Abs. 4 KDO.
- Für die Rechtmäßigkeit einer Übermittlung an kirchliche oder staatliche Stellen trägt die übermittelnde Stelle die Verantwortung, es sei denn sie erfolgt auf ausdrückliches Ersuchen der empfangenden Stelle. In diesem Fall ist nur die Schlüssigkeit des Ersuchens zu prüfen - . § 11 Abs. 2 KDO.
- Die Übermittlung von Daten an die Arbeitsagenturen ist durch Gesetz geregelt. Rechtsgrundlage ist hier z.B. § 86 SGB III
- Die Weitergabe personenbezogener Daten an privatrechtliche Empfänger ist ebenfalls möglich, wenn es zur Aufgabenerfüllung der übermittelnden Stelle erforderlich ist (§ 12 Abs. 1 Nr. 1 KDO) oder der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten dargelegt hat und kein schutzwürdiges Interesse des Betroffenen entgegensteht (§ 12 Abs. 1 Nr. 2 KDO). Berechtigt ist das Interesse des Datenempfängers dann, wenn es rechtlich schützenswert ist. Wirtschaftliche Gründe allein reichen hierfür nicht aus.
- Die Verantwortung für die Zulässigkeit einer Übermittlung an private oder gewerbliche Empfänger trägt nach § 12 Abs. 2 KDO immer die übermittelnde Stelle!

Einzelfälle:

Die Weitergabe von Daten zu Werbezwecken oder an die Presse liegt nicht im Aufgabenbereich der Bildungseinrichtungen. Ein berechtigtes, also rechtlich schützenswertes Interesse des Empfängers an der Kenntnis dieser Daten, besteht ebenfalls nicht. Eine Übermittlung kann daher nur mit ausdrücklicher und schriftlicher Zustimmung der Betroffenen erfolgen.

Öffentliche Stellen, Arbeitgeber, etc. haben ihre Daten ebenfalls direkt bei den Teilnehmern zu erheben. Die Bildungseinrichtungen haben insoweit keine Auskünfte zu erteilen. Dabei ist besondere Wachsamkeit angezeigt. Fälle, in denen Arbeitgeber nur nachgefragt haben, weil der Teilnehmer zur gleichen Zeit am Arbeitsplatz krank gemeldet war, machen deutlich, dass hier die Rechte der Betroffenen massiv beeinträchtigt werden können. Anderes kann allerdings dann gelten, wenn die Teilnahme auf Veranlassung dieser Stelle erfolgt und von dieser auch finanziert wird.

Die Veröffentlichung personenbezogener Daten der Referenten im Internet ist vorher mit diesen abzusprechen. In vielen Fällen macht es Sinn, den Referenten kurz mit seiner derzeitigen Position und beruflichen Qualifikationen vorzustellen. Diese Daten sind aber über Suchmaschinen, wie Google weltweit verfügbar. Deshalb bedarf ihre Veröffentlichung der Zustimmung der Betroffenen.

III. Datenspeicherung

Speichern ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger, § 2 Abs. 4 Nr. 1 KDO. Mit Datenträgern sind nicht nur elektronische Speichermedien gemeint, sondern auch Akten und Karteikarten. Hierfür gilt:

- Es dürfen nur solche Daten gespeichert werden, deren dauerhafte Aufbewahrung zur Aufgabenerfüllung notwendig ist, § 10 Abs. 1 KDO.
- Automatisiert gespeicherte Daten, die nicht mehr erforderlich sind, sind zu löschen. Gesetzliche Aufbewahrungsfristen sind dabei zu beachten, § 14 Abs. 2 Nr. 1 KDO.
- Die gespeicherten Daten dürfen nur für die Zwecke genutzt werden, für die sie erhoben worden sind, § 10 Abs. 1 KDO. Ausgenommen ist nach § 10 Abs. 3 KDO die Verwendung der Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen (Controlling, Prüfungen zur Qualitätssicherung, Zertifizierungsverfahren).

Besondere Arten personenbezogener Daten, § 2 Abs. 10 KDO

Hierzu gehören Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Sie sind in besondere Weise geschützt. Ohne Einwilligung des Betroffenen dürfen sie nach nur erhoben (§ 9 Abs. 5 KDO) und gespeichert (§ 10 Abs. 5 KDO) werden, wenn eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses, zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten, zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit, der Gesundheitsvorsorge, der

Durchführung wissenschaftlicher Forschung oder der Begründung und Durchführung eines Arbeitsverhältnisses zwingend erforderlich ist.

Die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen und schriftlich erteilt werden - § 3 Abs. 2 KDO.

IV. Technisch-organisatorische Maßnahmen

Gemäß § 6 KDO hat jede verantwortliche Stelle, die technischen und organisatorischen Maßnahmen zu treffen, die zum Schutz der Daten erforderlich sind. Folgende Maßnahmen dürften als Mindestanforderungen gelten:

- Eindeutige Regelung von Zuständigkeiten und Verantwortlichkeiten
- Festlegung der Lösungsfristen und Lösungsbeugnisse
- Verpflichtung der Mitarbeiter auf das Datengeheimnis, § 4 KDO
Das Datengeheimnis verpflichtet die Mitarbeiter nicht nur, über das, was ihnen im Rahmen ihrer dienstlichen Tätigkeit bekannt geworden ist, zu schweigen, sondern auch Daten nicht unbefugt zu erheben, zu verarbeiten oder zu nutzen.
- Belehrung der Mitarbeiter über ihre Pflichten.
- Maßnahmen zum Schutz der Datenträger (Akten, EDV) vor Beschädigung, Zerstörung und Verlust. Datensicherung
- Maßnahmen zum Schutz der Daten vor nicht autorisierter Einsichtnahme. Beachtung des Trennungsgebotes. Jedem Mitarbeiter darf nur den Teil des Gesamtdatenbestandes zur Verfügung gestellt werden, den er zur Erfüllung seiner Aufgaben benötigt.
- Beschreibung der eingesetzten Verfahren und Meldung an den Diözesandatenschutzbeauftragten, § 3a KDO
- Einbeziehung des Datenschutzes vor der Installation neuer Verfahren
- Gegebenenfalls Bestellung eines betrieblichen Datenschutzbeauftragten, §§ 18a, 18b KDO

Beim Einsatz von EDV zur personenbezogenen Datenverarbeitung sind besondere Sicherheitsmaßnahmen zu beachten. Auch hier können in diesem Rahmen nur Mindestanforderungen aufgeführt werden:

- Strikte Trennung der Verwaltungsrechner von den zur Schulung eingesetzten PCs.
- Rechteverwaltung bei Netzwerkbetrieb oder gemeinschaftlicher Nutzung eines Arbeitsplatzrechners.
- Zugriffsschutz durch Passwortvergabe, möglichst in Verbindung mit Chipkarte oder biometrischen Verfahren.
- Bei mobilen Datenverarbeitungsgeräten (Notebooks, Subnotebooks, Netbooks): Verschlüsselung der Festplatte. Mobile Geräte sind in besonderer Weise gefährdet, wenn es um Verlust oder Diebstahl geht. Daher muss verhindert werden, dass ein unrechtmäßiger Besitzer imstande ist, die Daten auszulesen.
- Regelmäßige, möglichst automatisierte Datensicherung. Einsatz von RAID-Systemen.
- Einsatz von Firewall und Virenschutzprogrammen bei Internet-Zugang.
- Übermittlung personenbezogener Daten über ungeschützte Internetzugänge oder E-Mail nur bei Verschlüsselung des Inhalts.

- Schriftliche Benutzerordnung für den Umgang mit EDV, Internet und E-Mail. Regelung insbesondere der Privatnutzung von Internet und E-Mail durch Mitarbeiter.

Die Veröffentlichung personenbezogener Daten im Internet bedarf besonderer Sorgfalt. Ohne Zustimmung des Mitarbeiters ist sie nur gestattet, wenn sie zur Aufgabenerfüllung zwingend erforderlich ist. Etwa dann, wenn eine Tätigkeit ohne Außenkontakt nicht möglich ist. Die Veröffentlichung von Fotos bedarf, wegen des nach § 23 Kunsturhebergesetz geschützten Rechts am eigenen Bild immer der Zustimmung der Betroffenen.

Die Zukunft hat schon begonnen: Augmented Reality

Stellen Sie sich vor, jemand beobachtet Sie, während Sie im Café sitzen. Während Sie genussvoll Ihre heiße Schokolade trinken und nichts Böses ahnen, nimmt Ihr Gegenüber sein Smartphone und fotografiert Sie. Über die Gesichtserkennung bekommt er anschließend eine Nachricht auf sein Gerät, die ihm sagt, dass es sich bei der fotografierten Person um „Peter Mustermann“ handelt, der für die Caritas arbeitet und mit zwanzig weiteren Personen soziale Kontakte unterhält. Woher Ihr Gegenüber das weiß? Suchsysteme haben Ihr Foto im Internet gefunden und einen Abgleich mit dem aufgenommenen Bild durchgeführt. Gleichzeitig hat das Suchsystem auch die Online-Communities nach Ihrer Person durchforstet und Sie bei Facebook gefunden. Diese Technik ist heute schon Wirklichkeit.

V. Besondere Verfahren

Auftragsdatenverarbeitung, § 8 KDO

„Outsourcing“ erfreut sich heute, meist durch den Zwang zu Einsparungen, großer Beliebtheit. In § 8 KDO wurde daher eine spezielle Rechtsgrundlage hierfür geschaffen. Dabei sind folgende Punkte zu beachten:

- Der Auftragnehmer ist nicht selbständiger Dritter im Sinne der Datenschutzvorschriften. Er ist hinsichtlich der Erhebung, Verarbeitung und Nutzung der Daten weisungsgebunden, § 8 Abs. 3 KDO
- Der Auftraggeber bleibt, auch haftungsrechtlich, in vollem Umfange verantwortlich, § 8 Abs. 1 KDO. Die Verantwortung kann also nicht delegiert werden!
- Wichtig ist daher eine besonders sorgfältige Auswahl des Auftragnehmers sowie die genaue schriftliche Festlegung der angewandten Verfahren, der Maßnahmen zu ihrem Schutz und etwaiger Unterauftragsverhältnisse. Personenbezogene Daten dürfen nicht ohne besondere Vorkehrungen in Drittländer übermittelt und dort gespeichert werden. Daher ist im Vertrag auch der Ort der Speicherung (Standort des Servers) festzulegen. Er sollte möglichst im Inland stehen, keinesfalls aber in einem Land, das keine Datenschutzbestimmungen und Aufsichtsbehörden auf diesem Gebiet kennt (unsicheres Drittland). Verstöße gegen die vertraglichen Pflichten oder gegen Weisungen des Auftraggebers sollten mit einer Vertragsstrafe belegt sein. In jedem Fall bedarf es eines zweiseitigen Vertrages. Eine einseitige „Datenschutzerklärung“ des Auftragnehmers reicht nicht aus.
- Die vorgenannten Grundsätze gelten auch dann, wenn es sich „nur“ um Wartungsarbeiten handelt, bei denen der Auftragnehmer die Möglichkeit hat, personenbezogene Daten einzusehen.

Videoüberwachung, § 5a KDO

Eine Rechtsgrundlage für die Durchführung von Überwachungsmaßnahmen mit optisch-elektronischen Einrichtungen ist nur für öffentlich zugängliche Räume vorhanden. Öffentlich sind Räume dann, wenn sie von einer unbestimmten Zahl von Personen betreten werden können. Das Betreten von Seminarräumen ist in der Regel nur den Teilnehmern, Referenten und Servicepersonal gestattet. Sie sind daher nicht öffentlich. Anders sieht es aus, wenn es um den Eingangsbereich oder das Grundstück selbst (z.B. Parkplatz) handelt. Auch solch ein öffentlicher Bereich darf nur dann videoüberwacht werden, wenn folgende Voraussetzungen vorliegen:

- Es muss ein Anordnungsgrund vorliegen, der die Einrichtung der Videoüberwachung erforderlich macht. Solche Gründe können sein:
 - Eingangskontrolle. Hier sind sowohl solche Systeme gemeint, die den gesamten Eingangsbereich erfassen, wie auch Kameras, die eine Gesichtskontrolle nach Betätigung der Türglocke ermöglichen.
 - Schutz vor Diebstahl.
 - Schutz vor Vandalismus.
 - Mitarbeiterüberwachung. Hierfür ist jedoch in jedem Fall eine Betriebsvereinbarung erforderlich. Eine generelle „Rund-um-die-Uhr-Überwachung“ verletzt jedoch in schwerwiegender Weise das Persönlichkeitsrecht der Betroffenen und ist daher generell unzulässig.
- Der Anordnungsgrund muss konkret festgelegt werden. Die erhobenen personenbezogenen Daten dürfen nur zum Erreichen des festgelegten Zieles genutzt werden. Auch hier gilt die strenge Zweckbindung.
- Auf den Umstand der Beobachtung muss deutlich erkennbar hingewiesen werden. Es muss zudem erkennbar sein, wer die Videoüberwachung angeordnet hat. Beispiel:
„Unsere Einrichtung wird videoüberwacht. Der Veraltungsleiter.“
Eine verdeckte Videoüberwachung ist nur in schwerwiegenden Fällen zulässig, in denen der Anordnungszweck auf andere nicht Weise erreicht werden kann.
- Bei Aufzeichnung dürfen die Daten nur solange aufbewahrt werden, wie sie zur Erreichung des Zwecks erforderlich sind. In der Regel sind das nicht mehr als 72 Stunden. Innerhalb dieses Zeitraums sollten sich Aufzeichnungsgeräte (Bänder, Festplatten) selbst überschreiben.
- Der Zugang zu den Aufzeichnungsgeräten und die Möglichkeit ihrer Auswertung und Verwendung muss personell klar geregelt sein.
- Die Videoüberwachung gehört mit zu den Verfahren automatisierter Datenverarbeitung, die vor ihrer Inbetriebnahme dem Diözesandatenschutzbeauftragten gem. § 3a KDO zu melden sind.

Wann ist eine Videoüberwachung sinnvoll?

- Eine Verhinderung von Straftaten wie Diebstahl und Sachbeschädigung ist in der Regel nur bei dauerhafter Beobachtung und kurzfristiger Reaktionsmöglichkeit zu erreichen.
- Die Aufzeichnung der Videoaufnahmen kann im günstigsten Fall Hinweise zur Ermittlung des Täters liefern. Dies ist aber abhängig von den Rahmenbedingungen, wie der Qualität der Kameras, ihrer Anbringung, des jeweils optisch erfassten Bereichs sowie ausreichender Beleuchtung.

- Meist sind weitere „flankierende“ Maßnahmen, wie ordnungsgemäße Raum- und Objektsicherung, Einsatz einer Warnanlage, Bewegungsmelder, etc. erforderlich. Hier sollten zuvor auch polizeiliche Beratungsstellen in Anspruch genommen werden.
- Untersuchungen zeigen, dass die Einrichtung einer Videoüberwachung üblicherweise spontan begangene Taten nicht verhindern kann. Solche Täter lassen sich im Moment von ihrem Impuls leiten und denken nicht darüber nach, ob sie sich im Erfassungsbereich einer Videokamera befinden. Beispiel: Der jüngste Fall in der Münchner U-Bahn, in der ein Helfer von alkoholisierten Jugendlichen zu Tode geprügelt wurde.
- Untersuchungen zeigen aber auch, dass geplante Straftaten in bestimmten Fällen signifikant zurückgehen. Täter scheuen das Risiko. Der Tatort wird meist vorher „ausbaldovert“. Dabei wird die Videoüberwachung als deutliche Risikoerhöhung wahrgenommen.
- Zum Erreichen des Abschreckungszwecks reicht in vielen Fällen schon die Anbringung von Attrappen aus.

VI. Rechte der Betroffenen

Mit jeder Änderung der Datenschutzvorschriften, wurden die Rechte der Betroffenen gestärkt. Nach dem derzeitigen Rechtsstand sind folgende Rechte zu gewähren:

- § 13 KDO - Anspruch auf Auskunft.
Der Betroffene hat zunächst die Möglichkeit, zu erfahren, was über ihn gespeichert wird, zu welchen Zwecken diese Daten verwendet und an wen sie regelmäßig übermittelt werden.
- § 13a KDO – Anspruch auf Benachrichtigung
Sind die Daten ausnahmsweise ohne seine Kenntnis erhoben worden, so ist er über die Speicherung, Zweckbestimmung, Verarbeitung oder Nutzung der Daten, unter Angabe der hierfür verantwortlichen Stelle zu unterrichten. Diese Verpflichtung entfällt nur dann, wenn der Betroffene bereits auf andere Weise Kenntnis erlangt hat, die Unterrichtung unverhältnismäßigen Aufwand erfordern würde oder durch eine gesetzliche Vorschrift ausdrücklich vorgesehen ist.
- § 14 Abs. 1 KDO - Anspruch auf Berichtigung.
Unrichtige oder unrichtig gewordene Daten sind zu berichtigen. Ist die Berichtigung bestritten, so sind die Daten zu sperren. Sie bleiben zwar gespeichert, dürfen aber nicht mehr genutzt werden. Stellen, an die diese Daten übermittelt worden sind, sind von der Berichtigung oder Sperrung zu verständigen, § 14 Abs. 8 KDO
- § 14 Abs. 2 KDO - Anspruch auf Löschung
Werden Daten unberechtigter Weise gespeichert oder sind sie in Zukunft nicht mehr erforderlich, so sind sie zu löschen. Die Erforderlichkeit bleibt mindestens solange bestehen, wie gesetzliche Aufbewahrungsfristen ihre Speicherung verlangen (z.B. steuerrechtliche Vorschriften).
- § 14 Abs. 5 KDO – Widerspruchsrecht
Einer Verarbeitung seiner Daten in elektronischer Form kann der Betroffene widersprechen. In diesem Fall ist zu prüfen, ob das schutzwürdige Interesse des Betroffenen, das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt.
- Gegen eine unberechtigte Weitergabe von Daten besteht ein Unterlassungs- und gegebenenfalls auch Schadensersatzanspruch nach § 823 BGB.
- § 5 Abs. 1 KDO – Unabdingbarkeit

Auf die Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung der Daten kann nicht durch Rechtsgeschäft verzichtet werden.

- § 15 KDO - Petitionsrecht

Der Betroffene hat jederzeit das Recht, sich mit einer Beschwerde an die zuständige Aufsichtsinstanz, den Diözesandatenschutzbeauftragten zu wenden.

Weitere Informationen:

- Sekretariat der Deutschen Bischofskonferenz (Hrsg.), Datenschutz und Melderecht der katholischen Kirche 2006. Arbeitshilfen Nr. 206, Bonn 2006
- Sekretariat der Deutschen Bischofskonferenz (Hrsg.), Internetpräsenz. Arbeitshilfen, Nr. 234, Bonn 2009

Beide Schriften können als gedruckte Ausgabe unmittelbar bei der Deutschen Bischofskonferenz bestellt werden. Ein elektronisches Formular hierfür findet sich hier:

<http://www.dbk.de/schriften/arbeitshilfe/index.html#>

Darüber hinaus können die Broschüren auch als PDF-Datei direkt heruntergeladen und im Bedarfsfall ausgedruckt werden. Die Dateien zum Download finden Sie hier:

<http://www.dbk.de/schriften/arbeitshilfe/index.html#>

<http://www.datenschutz-kirche.de/download/ah206.pdf>

http://www.datenschutz-kirche.de/download/ah_234.pdf