Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Arbeitshilfe
AH 100

Einführung in das Datenschutzrecht der katholischen Kirche
Eine Erstinformation für Mitarbeiter

im Erzbistum Hamburg,
den Bistümern Hildesheim und Osnabrück
und dem Bischöflich Münsterschen Offizialat in Vechta i.O.

Stand: 03/2018

Herausgegeben vom

Diözesandatenschutzbeauftragten
des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

Unser Lieben Frauen Kirchhof 20
28195 Bremen

Tel.: 0421 / 16 30 19 25
Mobil: 0151 / 41 97 57 58
Mail: info@datenschutz-katholisch-nord.de

Diese Arbeitshilfe können Sie auch auf unserer Internetseite abrufen unter:
https://www.datenschutz-kirche.de/

Inhaltsverzeichnis

Das Anliegen dieser Schrift

Durch Erlass des Gesetzes über den kirchlichen Datenschutz (KDG) hat die katholische Kirche ihr Datenschutzrecht in Übereinstimmung mit der Datenschutz-Grundverordnung der Europäischen Union vollständig neu geregelt. Was ändert sich hierdurch? Es wurde ein modernes und zeitgemäßes Recht geschaffen, das dem Einzelnen eine faire Verwendung seiner Daten und den Schutz seines Persönlichkeitsrechts erhalten soll. Damit das im digitalen Zeitalter noch gelingen kann, sind die Vorschriften zur Einhaltung datenschutzgerechter Verarbeitungen wesentlich verschärft worden. Zugleich wurden auch den Aufsichtsbehörden Maßnahmen an die Hand gegeben, die eine effektive Durchsetzung der Rechte der betroffenen Personen ermöglichen sollen. Hierzu dient insbesondere das Anordnungsrecht, das in § 47 Absatz 5 KDG festgelegt wurde und in entsprechenden Fällen zu einer Beschränkung oder gar dem Verbot der Datenverarbeitung führen kann. Darüber hinaus besteht auch die Möglichkeit den vorsätzlichen oder fahrlässigen Verstoß gegen Bestimmungen des Gesetzes mit Geldbußen bis 500.000 Euro zu ahnden. Der Datenschutz kann daher nicht mehr als „Papiertiger“ angesehen werden, sondern er ist als ein wirksames Mittel zur Durchsetzung einer Verarbeitung, die auf das Persönlichkeitsrecht von Menschen Rücksicht nimmt.

Die in den Einrichtungen tätigen Mitarbeiterinnen und Mitarbeiter müssen daher auf das neue Recht vorbereitet und geschult werden. Zu groß ist sonst die Gefahr, dass durch Beanstandungen, Anordnungen und Geldbußen, die Glaubwürdigkeit ihres Dienstes sowohl im innerkirchlichen Bereich, wie auch nach außen hin, erheblich beschädigt wird.

Diese Schrift will daher dazu beitragen, dass alle Mitarbeiter, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, die Grundregeln des Datenschutzes in der neuen Form kennen. Deshalb sollte diese Arbeitshilfe auch denjenigen zur Verfügung gestellt werden, die zuvor bereits die 1. Auflage von Oktober 2015 durchgearbeitet haben.

Zur bisher geltenden KDO ist zugleich „Die Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)“ erlassen worden. Diese bleibt bis zu ihrem Neuerlass, spätestens aber bis zum 30. Juni 2019 in Kraft, wie es in § 57 Abs. 5 KDG bestimmt wird. Dort ist in Ziffer II Abs. 1 Nr. 1 geregelt, dass alle kirchlichen Dienststellen und Einrichtungen verpflichtet sind, ihre bei der Verarbeitung personenbezogener Daten tätigen Mitarbeiterinnen und Mitarbeiter mit den Datenschutzvorschriften vertraut zu machen. Die Verpflichtung, die Mitarbeiterinnen und Mitarbeiter mit den Vorschriften des KDG sowie anderer Vorschriften über den Datenschutz vertraut zu machen, obliegt nach § 38 S. 3 lit. c) KDG dem betrieblichen Datenschutzbeauftragten.

Diese Verpflichtung gilt somit weiterhin für alle Einrichtungen, die nach § 3 Absatz 1 KDG das kirchliche Datenschutzrecht anzuwenden haben, also die gesamte verfasste Kirche, die Caritas und sonstige kirchliche Körperschaften, jeweils unabhängig von ihrer Rechtsform.

Vertraut machen bedeutet dabei mehr, als den Mitarbeiterinnen und Mitarbeitern den Wortlaut des KDG und weiterer geltenden Vorschriften zugänglich zu machen. Vielmehr ist dafür Sorge zu tragen, dass diese fähig werden, ihre Verpflichtung aus § 5 KDG zur Wahrung des Datengeheimnisses zu erfüllen. Hiernach ist es ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten. Sie sind auf die Einhaltung der datenschutzrechtlichen Vorschriften zu verpflichten und müssen das Datengeheimnis auch über das Ende ihrer Tätigkeit hinaus wahren. Diese Anforderung kann aber nur dann erfüllt werden, wenn sie zuvor über die wesentlichen Grundsätze und Ziele des Datenschutzes belehrt worden sind, wie es in der Ausführungsvorschrift, der KDO-DVO festgelegt ist.

Mitarbeiterinnen und Mitarbeiter, die unter der unmittelbaren Verantwortung des Verantwortlichen zur Verarbeitung personenbezogener Daten befugt sind, gehören zum privilegierten Teil der bei der Datenverarbeitung tätigen Personen. Sie sind daher auch für die Wahrung der Rechte der betroffen Personen mitverantwortlich.

Nach § 51 Absatz 6 KDG können gegen kirchliche Stellen, die öffentlich-rechtlich verfasst sind, keine Geldbußen verhängt werden. Diese Ausnahme gilt aber nur für die „Stellen“ und entlastet nicht die dort Beschäftigten, wenn sie datenschutzrechtliche Regeln vorsätzlich oder fahrlässig verletzt haben!

Die nachfolgenden Kapitel wollen deshalb dazu beitragen, all denjenigen, die mit der Datenverarbeitung in unseren Einrichtungen betraut sind, einen ersten Überblick zu verschaffen, was nach dem neuen Recht zu einem datenschutzfreundlichen Verhalten gehört. Die Wahrung des Persönlichkeitsrechts der betroffenen Person und ihres legitimen Anspruchs auf informationelle Selbstbestimmung muss für kirchliche Dienststellen selbstverständlich sein.

Gleichzeitig sollen alle Dienstvorgesetzten in ihrer Aufgabe, die Mitarbeiterinnen und Mitarbeiter über ihre Pflichten zu belehren, aktiv unterstützt werden. Die gegebenenfalls festzustellende Notwendigkeit zu weiteren Fortbildungsmaßnahmen wird hierdurch nicht beseitigt.

Diese Schrift kann selbstverständlich nicht alle Fragen beantworten, die sich aus der täglichen Praxis heraus ergeben können. Sie stellt jedoch einen Einstieg dar, der zu einem ver-

stärkten Problembewusstsein und zu weiteren Nachfragen in kritischen Situationen führen soll.

Bremen, im März 2018

Einführung

Sie sind Mitarbeiterin oder Mitarbeiter der katholischen Kirche. Sie haben es sich zur beruflichen Aufgabe gemacht, Menschen durch ihren christlichen Dienst zu helfen. Dabei sind sie zumeist in den Bereichen der Verkündigung, der Lehre oder der Diakonie tätig. Sie erfahren immer wieder, dass ihre Arbeit ein hohes Maß an Vertrauen voraussetzt. In der Kirche wird daher schon seit langer Zeit das Beicht- und Seelsorgegeheimnis gewahrt, auf dessen Einhaltung die betroffenen Personen vertrauen. Darüber hinaus bestehen weitere Verschwiegenheitspflichten. Beispielsweise für Sozial- und Personaldaten. Für bestimmte Berufe hat der Gesetzgeber eine Verschwiegenheitspflicht über Privatgeheimnisse einzelner Personen verfügt und durch einen Straftatbestand in § 203 StGB abgesichert. Dies gilt unter anderem für Ärzte, Angehörige anderer Heilberufe, Berufspsychologen, Ehe-, Familien-, Erziehungs- oder Jugendberater, Berater für Suchtfragen, Mitglieder einer Schwangerschaftsberatungsstelle sowie staatlich anerkannte Sozialarbeiter oder Sozialpädagogen und deren Gehilfen.

Aber die Erfüllung dieser Verschwiegenheitspflichten reicht in der heutigen Zeit allein nicht mehr aus. Das Bundesverfassungsgericht hat festgestellt, dass jedem Menschen ein Recht auf „informationelle Selbstbestimmung“ zustehe. „*Jeder müsse daher selbst darüber entscheiden können, wer, wann, was und bei welcher Gelegenheit über ihn weiß*“ (BVerfG Urt. vom 15.12.1983). Dieses Grundrecht setzt also schon zu einem sehr viel früheren Zeitpunkt an. Es erfasst auch die Erhebung, Verarbeitung und Nutzung personenbezogener Daten oder ganz einfach ausgedrückt: die Schweigepflicht entscheidet nur darüber, welche Daten ich weitergeben darf oder für mich behalten muss, der Datenschutz regelt, ob ich diese Daten überhaupt kennen und im dienstlichen Bereich für eigene Zwecke weiterverarbeiten darf.

Dieses Grundrecht ist heute europaweit anerkannt. So legt die Charta der Grundrechte der Europäischen Union in Art. 8 fest:

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Der Wortlaut dieses Grundrechts spricht von „personenbezogenen Daten“. Der Begriff wird in § 4 Nr. 1 KDG definiert. Es muss sich um Daten handeln, die sich auf eine natürliche Person beziehen. Die Informationen über juristische Personen (Firmen, Verwaltungsstellen, Vereine, Verbände, Genossenschaften, Stiftungen, und andere) fallen nicht unter den Schutz des Art. 8 der Grundrechtscharta. Die Daten müssen außerdem einer natürlichen Person zurechenbar sein. Das ist nur dann der Fall, wenn die betroffene Person bekannt ist oder ihre Identität festgestellt werden kann. Letzteres ist zum Beispiel auch dann der Fall, wenn ohne Namensnennung anhand bestimmter Kriterien ermittelt werden kann, auf welche Person die Informationen zutreffen („Die Person über die ich spreche, hat ein besonders auffälliges Muttermal am rechten Arm…“, jeder der den Menschen mit dieser Auffälligkeit kennt, weiß Bescheid.). Bei der Kennzeichnung von Personengruppen handelt es sich dann um personenbezogene Daten, wenn erkennbar ist, wer der Gruppe angehört und die Tatsachen auf ihn „durchschlagen“. Zum Beispiel wenn eine betroffene Person aufgrund statistischer Werte als Mitglied einer bestimmten „Käuferschicht“ eingestuft und auch so behandelt wird. Der Datenschutz greift immer dann ein, wenn Informationen einem Menschen direkt oder indirekt zurechenbar sind. In diesem Falle wird er durch die Verarbeitung in seinem Persönlichkeitsrecht beeinträchtigt.

Auf der anderen Seite können Sie Ihre Aufgabe nur dann erfüllen, wenn sie über die Person, die Sie betreuen auch etwas wissen. Das informationelle Selbstbestimmungsrecht gilt daher nicht uneingeschränkt. Es kann durch Rechtsvorschriften eingeschränkt werden, um eine ordnungsgemäße Bearbeitung dienstlicher Aufgaben zu ermöglichen. In § 6 Abs. 1 KDG sind die Voraussetzungen hierzu verpflichtend festgestellt. Liegen diese Voraussetzungen nicht vor, kann die Datenverarbeitung nur mit der Einwilligung der betroffenen Person vorgenommen werden.

Eine erlaubte Datenverarbeitung muss weiterhin die in § 7 KDG festgelegten Grundsätze beachten. Sie muss vor allem nachvollziehbar sein und darf nur für bestimmte, festgelegte Zwecke erfolgen (Zweckbindung). Außerdem muss gewährleistet werden, dass die verarbeiten Daten sachlich richtig und auf dem neuesten Stand sind (Integrität der Datenbestände). Auch die Sicherheit vor unbefugter Benutzung oder Verarbeitung (Vertraulichkeit) muss genauso gewährleistet sein, wie ein Schutz vor unbeabsichtigtem Verlust oder gar Zerstörung (Bestandsgarantie).

Die Verpflichtung, technisch-organisatorische Maßnahmen zur Sicherung des Datenbestandes zu treffen ist in § 26 KDG geregelt. Von den Mitarbeiterinnen und Mitarbeitern wird verlangt, dass sie einmal festgelegte Maßnahmen kennen und einhalten. Ohne ihre ordnungs-

gemäße Umsetzung im Büroalltag ist ein Schutz der betroffenen Personen nicht zu erreichen.

Deshalb werden durch § 5 KDG alle in der Datenverarbeitung tätigen Personen auf das Datengeheimnis verpflichtet.

„Datengeheimnis

Den bei der Verarbeitung personenbezogener Daten tätigen Personen ist untersagt, diese unbefugt zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis und die Einhaltung der einschlägigen Datenschutzregelungen schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.“

Von Ihnen wird daher Folgendes erwartet

- Anordnung über das kirchliche Meldewesen (KMAO)
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft
- Anordnung über die Sicherung und Nutzung der kirchlichen Archive (KAO)
- Ordnung zur Prävention von sexualisierter Gewalt an Kindern, Jugendlichen und Erwachsenen Schutzbefohlenen (PrävO)

Die Grundprinzipien des Datenschutzes nach dem KDG

I. Rechtmäßigkeit der Datenverarbeitung

Der Begriff der Datenverarbeitung ist in § 4 Nr. 3 KDG erläutert. Im Gegensatz zu früher wird hiermit jetzt die gesamte Tätigkeit des Umgangs mit personenbezogenen Daten erfasst. Angefangen von der Erhebung über das Erfassen, die Speicherung, das Nutzen, die Offenlegung bis hin zur Organisation der Verarbeitungstätigkeit. Die frühere Unterscheidung zwi-

schen Erhebung, Verarbeitung und Nutzung, wie sie von der bisher geltenden KDO vorgenommen worden ist, wurde in Übereinstimmung mit der Datenschutzgrundverordnung aufgegeben.

Die Vornahme einer Datenverarbeitung führt immer zu einer Einschränkung der Rechte der Menschen, selbst darüber zu bestimmen, wer, wann, was und bei welcher Gelegenheit über sie wissen darf. Die Verarbeitung personenbezogener Daten ist daher nur zulässig, wenn sie von einer gesetzlichen Grundlage gestattet oder gar angeordnet wird oder die betroffene Person in die Verarbeitung eingewilligt hat (§ 6 Abs. 1 KDG). Es handelt sich also, wie bisher, um ein generelles Verbot mit Erlaubnisvorbehalt. Dies gilt nicht nur für eine automatisierte Verarbeitung sondern auch für den Fall einer nichtautomatisierten Verarbeitung, soweit sie in einem Dateisystem gespeichert wird (§ 2 Abs. 1 KDG). Hierzu definiert § 4 Nr. 8 KDG das Wort „Dateisystem“ als eine strukturierte Sammlung von Daten, die nach bestimmten Kriterien zugänglich sind. Dabei kommt es nicht darauf an, ob die Zuordnung zentral, dezentral, nach funktionalen oder geografischen Gesichtspunkten erfolgt. In jedem Fall trifft diese Definition auf Akten, Aktensammlungen und Karteikarten zu.

1. Vorliegen einer gesetzlichen Erlaubnis

Am Anfang steht also die Frage, ob in all diesen Fällen, für die durchgeführte oder geplante Verarbeitung personenbezogener Daten eine der Zulässigkeitsvoraussetzungen gegeben ist. Dabei ist zunächst zu überlegen, ob sie durch das KDG oder eine andere kirchliche oder staatliche Rechtsvorschrift erlaubt ist.

Sie sind in ganz unterschiedlichen Bereichen kirchlicher Aufgaben tätig. Für jeden, der Verantwortung trägt, ist es ganz selbstverständlich nötig, die Rechtsvorschriften zu kennen, auf deren Basis ihre Arbeit erfolgt. Wer zum Beispiel in der Pflege tätig ist, muss sich durch Kenntnis des Sozialgesetzbuchs, Teil XI über die Bedingungen und Anforderungen seines Berufes unterrichten. Für Krankenhäuser gibt es bereichsspezifische kirchliche Datenschutzbestimmungen, ebenso wie für Schulen, Friedhöfe, das Meldewesen und Archive bis hin zur Präventionsordnung.

Übersicht über die in den norddeutschen Diözesen weiterhin geltenden bereichsspezifischen Vorschriften

- Anordnung über das kirchliche Meldewesen (KMAO)
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft
- Anordnung über die Sicherung und Nutzung der kirchlichen Archive (KAO)
- Ordnung zur Prävention von sexualisierter Gewalt an Kindern, Jugendlichen und erwachsenen Schutzbefohlenen (PrävO)

Darüber hinaus bestehen allgemeine staatliche Vorschriften, die teilweise auch für kirchliche Dienststellen zu beachten sind. Die Beispiele reichen hier vom Steuerrecht über das bereits genannte Sozialgesetzbuch (SGB V, VIII, XI), dem Bundesmeldegesetz (BMG), dem Telemediengesetz (TMG) bis hin zum Gesetz zur Kooperation und Information im Kinderschutz (KKG). Weitere Beispiele könnten angeführt werden, sie würden jedoch den Rahmen dieser Schrift sprengen. Bei jeder gesetzlichen Vorschrift wird auch der Umfang der erlaubten Datenverarbeitung angegeben, der selbstverständlich zu beachten ist. Hinsichtlich des Umfangs der Erhebung von Daten, der Dauer ihrer Speicherung und der Berechtigung sie anderen gegenüber offenzulegen, bestehen hier auch wesentliche Einschränkungen.

Wichtig ist es deshalb, dass sich jede Mitarbeiterin/jeder Mitarbeiter über die gesetzlichen Vorschriften informiert, die für die jeweilige Tätigkeit anzuwenden sind. In Zweifelsfällen sollten sie ihren Dienststellenleiter um nähere Angaben und Aufklärung bitten.

Weiterhin nennt § 6 Abs. 1 KDG eine Reihe von Gründen, die die Notwendigkeit einer Datenverarbeitung auch ohne die Einwilligung der betroffenen Person rechtfertigt. Hierbei handelt es sich um

- Die Gestaltung vertraglicher Beziehungen, einschließlich etwaiger Vorverträge (lit. c).
- Die Erfüllung rechtlicher Verpflichtungen des Verantwortlichen (lit. d).
- Der Schutz lebenswichtiger Interessen der betroffenen oder anderer Personen (lit. e).
- Die Wahrnehmung einer Aufgabe im kirchlichen Interesse oder der Ausübung öffentlicher Gewalt als Beliehener (lit. f KDG).

- Die Wahrung berechtigter Interessen des Verantwortlichen oder Dritter (lit. g).

Wichtig sind vor allem die beiden ersten Punkte. Vertragliche Beziehungen, wie arbeitsrechtliche Dienstverträge, Aufnahmeverträge für Kindertagesstätten und Schulen, Patientenverträge gehören beispielsweise hierzu. Nicht aber Bewerbungsunterlagen, da hier weder ein Dienstvertrag noch ein Vorvertrag mit dem Bewerber besteht. Sollen die Unterlagen auch noch für weitere Ausschreibungen genutzt werden, ist nach Ziffer 2 in diesem Kapitel zu verfahren und die Einwilligung der betroffenen Person einzuholen.

Bei der Erfüllung rechtlicher Verpflichtungen ist vorzugsweise an staatliche Aufzeichnungspflichten zu denken. Als Beispiel hierfür mag die Führung einer Spenderdatei dienen oder das namentliche Festhalten der Teilnehmer einer Fortbildungsveranstaltung, wenn dies zur Erlangung staatlicher Zuschüsse erforderlich ist.

Sind für Ihre Aufgabe keine gesetzlichen Regelungen der Kirche oder anwendbare staatliche Vorschriften erlassen worden, und liegt auch keine Erlaubnis im Sinne von Absatz 1 lit. c) bis g) vor, dürfen Sie die Datenverarbeitung nur mit Einwilligung der betroffenen Person vornehmen. Das Verfahren hierzu ist in § 8 KDG geregelt.

2. Einwilligung der betroffenen Person

Nach § 6 Abs. 1 lit. b) KDG dürfen personenbezogene Daten verarbeitet werden, wenn die betroffene Person hierin eingewilligt hat. Eine beachtenswerte Einwilligung liegt dann vor, wenn die Bedingungen nach § 4 Nr. 13 KDG und § 8 KDG erfüllt sind. Sie muss

- auf Grund einer freiwilligen Entscheidung der Person erfolgen (§ 8 Abs. 1 Satz 2);
- die jederzeit widerrufen werden kann (§ 8 Abs. 6);
- für einen bestimmten Fall abgegeben werden (§ 4 Nr. 13);
- in informierter Weise, das heißt nach Belehrung über den Zweck der Verarbeitung (§ 8 Abs. 1 Satz 1);
- bei Verlangen ist auf die Auswirkungen der Verweigerung hinzuweisen (§ 8 Abs. 1 Satz 1);
- eine eindeutige bestätigende Handlung sein, die in unmissverständlicher Form zu erkennen gibt, dass ein Einverständnis mit der geplanten Datenverarbeitung besteht (§ 4 Nr. 13);
- und zudem in schriftlicher Form abgegeben werden (§ 8 Abs. 2).

Es ist daher nicht ausreichend, wenn auf allgemeine vertragliche Erklärungen oder Geschäftsbedingungen hingewiesen wird. Hierbei fehlt es an der in § 4 Nr.13 KDG genannten Voraussetzung „für den bestimmten Fall“, da in diesen Bestimmungen nicht erkennbar wird, welche Daten für welche Zwecke verarbeitet werden sollen. Als Beispiel wird immer wieder angeführt, dass eine Kindertagesstätte oder eine Schule nicht Bilder der Kinder veröffentlichen darf, nur weil dies im Betreuungs- oder Schulvertrag allgemein genehmigt worden ist. Es muss vielmehr für bestimmte vorliegende Bilder die Einwilligung zu ihrer Verbreitung in namentlich bezeichneten Medien erfolgen.

Die Einwilligung kann von der betroffenen Person jederzeit widerrufen werden (§ 8 Abs. 6 Satz 1). Erfolgt ein solcher Widerruf, wirkt er nur für die Zukunft (§ 8 Abs. 6 Satz 2). Die vorher stattgefundene Datenverarbeitung bleibt rechtmäßig. Der Widerruf muss zudem genauso einfach möglich sein, wie die Erteilung desselben zuvor (§ 8 Abs. 6 Satz 3). Wird für die Einwilligungserklärung beispielsweise ein Formular benutzt, so kann in einem nachfolgenden Absatz auch ein Widerruf vorgesehen werden. Wird im Internet die Einwilligung durch das Ankreuzen einer entsprechenden Aufforderung erhoben, so muss dem Nutzer auch die Möglichkeit eingeräumt werden, sie durch ein weiteres Häkchen an gleicher Stelle zu widerrufen.

Die weitere Voraussetzung „für einen bestimmten Fall“ will erreichen, dass die betroffene Person genau unterrichtet wird, welche seiner personenbezogenen Daten an welcher Stelle verarbeitet werden sollen. Ebenso muss sie wissen, ob diese Daten an Dritte weitergegeben werden sollen und welche Empfänger in Frage kommen, sie zu erhalten. Diese Bedingung steht in direktem Zusammenhang mit der Belehrung über den Zweck der Verarbeitung. Daher ist auf Nachfrage der betroffenen Person dieser auch auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die genannten Aspekte sind maßgebliche Voraussetzung für eine informierte und freie Entscheidung des Einzelnen.

Zudem ist regelmäßig die Einwilligung in schriftlicher Form erforderlich. Einerseits wird hierdurch der Nachweis nach § 8 Abs. 5 erbracht, dass die betroffene Person mit der Verarbeitung ihrer Daten einverstanden ist, andererseits hat die Schriftform im deutschen Recht auch eine Appellfunktion, die Ernsthaftigkeit einer Erklärung wird hierdurch hervorgehoben. Eine mündliche Zusage hat in der Regel nicht den gleichen Grad an Verlässlichkeit.

Eine Einwilligungserklärung, die auf einer Internetseite abgegeben wird, muss auf dem Server des Anbieters so abgespeichert werden, dass sie im Bedarfsfall wieder aufgerufen werden und als Nachweis dienen kann.

Bei der elektronischen Verarbeitung werden Kinder und Jugendliche durch § 8 Abs. 8 KDG besonders geschützt. Hier besteht die besondere Gefahr, dass auch unvorteilhafte oder nicht passende Angebote allein mit einem Klick auf der Webseite angenommen werden. Auch eine Einwilligungserklärung ist mit einem Mausklick sehr schnell abgegeben, ohne dass in diesem Fall eine Informiertheit im zuvor geschilderten Sinne angenommen werden kann. Erst mit Vollendung des sechzehnten Lebensjahres gesteht man einem Heranwachsenden die Reife zu, seine Entscheidung auch in dieser Hinsicht allein treffen zu können. Bei allen jüngeren Personen ist die Datenverarbeitung nur dann rechtmäßig, wenn die Einwilligung der Sorgeberechtigten vorliegt. Eine besondere Schwierigkeit besteht in diesen Fällen darin, durch angemessene Anstrengungen, unter Einsatz verfügbarer Technik, das Alter der Person und die Rechtmäßigkeit der Einwilligungserklärung feststellen zu können. Das wird in der Regel nur durch die Einführung eines Double-Opt-in-Verfahrens zu gewährleisten sein. Es muss in diesen Fällen streng darauf geachtet werden, dass diese Voraussetzungen eingehalten werden.

Kostenfreie Beratungsangebote kirchlicher Dienststellen sind insoweit privilegiert, als hier die Altersgrenze verringert und auf das dreizehnte Lebensjahr festgelegt wurde. Damit soll auch die Möglichkeit bestehen, dass Kinder, die durch häusliche Konflikte gravierende Probleme haben, imstande sind, auch ohne Einwilligung ihrer Eltern Beratungsangebote in Anspruch nehmen können.

3. Rechtmäßigkeit einer Nutzung für andere Zwecke

Personenbezogene Daten werden meist bei der betroffenen Person selbst für einen bestimmten Verarbeitungszweck erhoben. Die betreffende Person weiß damit einerseits also, welche Aufgaben hiermit erfüllt werden sollen. Andererseits kann sich häufiger die Situation ergeben, dass die gleichen Informationen auch noch für andere Zwecke eingesetzt werden können, die den betroffenen Personen bei der Datenerhebung nicht mitgeteilt wurden. Hiermit würde aber das Recht des Einzelnen ausgehebelt, überschauen zu können, wer und zu welchen Zwecken über seine Daten verfügt. Deshalb hat der Datenschutz schon bisher dieser Nutzung einen Riegel vorgeschoben, der eine weitere Verwendung nur in Ausnahmefällen ermöglicht. Im KDG ist dies in § 6 Abs. 2 geregelt. Die Aufzählung der Möglichkeiten zwischen lit. a) bis j) ist abschließend. Weitere Ausnahmetatbestände bestehen nicht. Dies folgt aus der Formulierung des Gesetzestextes (Die Verarbeitung für einen anderen Zweck… ist nur rechtmäßig, wenn…). Gegenüber dem abgelösten Recht nach der KDO sind hier keine Änderungen erfolgt.

Wichtig ist noch der in § 6 Abs. 4 formulierte Grundsatz. Eine Zweckänderung, die nicht aufgrund einer Rechtsvorschrift (lit. a)) oder durch Einwilligung der Person (lit. b)) erfolgt ist nur dann rechtmäßig, wenn sie mit dem ursprünglichen Zweck vereinbar ist.

4. Rechtmäßigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung einiger besonderer Kategorien personenbezogener Daten unterliegt besonderen Bedingungen. Nach der Definition in § 4 Nr. 2 KDG handelt es sich hierbei um Daten

- über die rassische und ethnische Herkunft,
- über politische Meinungen,
- über religiöse oder weltanschauliche Überzeugungen,
- über die Gewerkschaftszugehörigkeit,
- über die in Nr. 15 beschriebenen genetischen Daten,
- über die in Nr. 16 beschriebenen biometrischen Daten, die zur eindeutigen Identifizierung einer natürlichen Person geeignet sind,
- über die in Nr. 17 beschriebenen Gesundheitsdaten,
- über Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Für eine öffentlich-rechtliche Religionsgesellschaft ist es in vielen Bereichen, vom Meldewesen über das Steuerrecht bis hin zur Personalführung notwendig von den betroffenen Personen ihre Zugehörigkeit zur Kirche zu kennen. Nicht verbunden mit dem Merkmal „r.k." ist jedoch ein sicheres Wissen über die von den Mitgliedern vertretenen religiösen oder weltanschaulichen Überzeugungen. Deshalb ist in § 4 Nr. 2 S. 2 KDG bestimmt, dass allein das Merkmal der Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft nicht zu der besonderen Kategorie personenbezogener Daten gehört. Die Frage, ob jemand eine Einführung des Priesteramts der Frau begrüßen würde, fällt allerdings unter die obige Definition.

Die Verarbeitung dieser Daten ist nach § 11 Abs. 1 KDG grundsätzlich untersagt. Deshalb können sie nur bei dem Vorliegen bestimmter Ausnahmetatbestände verarbeitet werden, die in § 9 Abs. 2 abschließend aufgezählt werden. Auf die ausführlichen Angaben unter lit. a) bis j) muss an dieser Stelle verwiesen werden. Absatz 4 der Vorschrift stellt zudem weitere, erhöhte Anforderungen an den technisch-organisatorischen Schutz dieser Daten.

Was wird von mir erwartet?

- Ich muss mich darüber informieren, welche Datenschutzvorschriften für meinen Tätigkeitsbereich erlassen worden sind.
- Ich muss die dort festgelegten Regeln in Bezug auf den Umfang der Datenerhebung und die Verarbeitung dieser Daten einhalten.
- Liegen keine rechtlichen Regelungen vor, darf ich die Daten nur mit freiwilliger und schriftlicher Einwilligungserklärung der betroffenen Person verarbeiten.

II. Grundsätze der Verarbeitung personenbezogener Daten

Da der Verantwortliche und seine Mitarbeiter im Hinblick auf die von ihnen eingesetzte Technik und deren Möglichkeiten, Daten schnell und unkompliziert auf verschiedene Stellen weltweit zu verteilen, ein großes Überlegenheitspotential gegenüber der betroffenen Person in Anspruch nimmt, muss hier ein Korrektiv geschaffen werden. Die Vorschrift des § 7 KDG ist also die entscheidende Norm zum rechtlichen Schutz der betroffenen Person. Auch hier hat man sich weitgehend an die schon bisher geltenden Bedingungen gehalten. Festgelegt wurden dabei

- Die Verpflichtung zu Rechtmäßigkeit und Transparenz (§ 7 Abs. 1 lit. a KDG).
- Die Verarbeitung nur für eindeutige und legitime Zwecke (§ 7 Abs. 1 lit. b KDG).
- Eine Datenminimierung und Pseudonymisierung, soweit sie erfolgen kann (§ 7 Abs. 1 lit. c KDG).
- Die sachliche Richtigkeit und Aktualität der Daten (§ 7 Abs. 1 lit. d KDG).
- Die Begrenzung der Dauer der Speicherung personenbezogener Daten (§ 7 Abs. 1 lit. e KDG).
- Eine angemessene Sicherheit durch den Schutz der Integrität und Vertraulichkeit, der verarbeiteten personenbezogenen Daten (§ 7 Abs. 1 lit. f KDG).

Nur dann, wenn diese Anforderungen erfüllt werden, können die betroffenen Personen auf die Wahrung ihrer Rechte vertrauen. Daher wird in § 7 Abs. 2 KDG zwingend festgelegt, dass

- der Verantwortliche zu einer Datenverarbeitungsorganisation gezwungen ist, bei der diese Bestimmungen beachtet werden,
- dass er hierfür die Verantwortung trägt und

- jederzeit imstande sein muss, dies nachzuweisen. Ein wesentlicher Bestandteil des Nachweises ist auf jeden Fall ein Verzeichnis der Verarbeitungstätigkeiten nach § 31 KDG.

1. Strenge Zweckbindung

Die rechtmäßig erhobenen Daten dürfen nach § 7 Abs. 1 lit. b) KDG immer nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Entscheidend ist dabei, dass sie nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Gesteht man der betroffenen Person das Recht zu erkennen zu können, für welche Aufgaben die Datenverarbeitung erfolgt, dann ist es selbstverständlich und folgerichtig, dass sie auch nur für den Zweck verwendet werden dürfen, für den sie erhoben worden sind.

Hat die betroffene Person nach § 15 KDG selbst bei der Erhebung der Daten mitgewirkt (unmittelbare Datenerhebung), so ist ihm auch mitgeteilt worden, wofür sie benötigt werden. Daher darf er auch darauf vertrauen, dass sie tatsächlich nur für die ihm mitgeteilten Zwecke genutzt werden. Sind im Einzelfall die Daten ohne ihn erhoben worden (§ 16 KDG – Mittelbare Datenerhebung), so muss er erst recht davor geschützt werden, dass diese zu allen möglichen Zwecken verwendet und ausgewertet werden und er schließlich nicht mehr überschauen kann, was alles und an welchen Stellen über ihn gewusst wird.

Nur dann, wenn diese Voraussetzungen erfüllt sind, kann die betroffene Person selbst wirklich frei darüber entscheiden, welche Informationen er über sich preisgeben will. Andernfalls wird er entweder die entsprechenden Angaben verweigern oder mit dem für ihn bedrückenden Gefühl leben müssen, nicht zu wissen, wer sonst noch Kenntnis dieser Daten erlangen wird und in welcher Weise diese gegen ihn verwendet werden können. Der Zweckbindungsgrundsatz ist daher einer der wichtigsten und entscheidendsten Grundlagen für den Datenschutz insgesamt.

Durchbrochen wird dieser Grundsatz nur in den Fällen, die abschließend in § 6 Abs. 2 lit. a) - j) KDG festlegt wurden.

2. Erforderlichkeit und Datensparsamkeit

Das KDG bestimmt, dass der Umfang der Daten auf das notwendige Maß zu beschränken ist (Grundsatz der Erforderlichkeit). In § 7 Abs. 1 lit. c) wird angeführt, dass sie dem Zweck angemessen und erheblich sein sollen.

Welche Daten sind aber erforderlich und dürfen daher erhoben, gespeichert und verarbeitet werden? Können die Dienststellen und Einrichtungen nach eigenem Belieben hierüber entscheiden? In vielen bereichsspezifischen Vorschriften finden sich Angaben über den Umfang der zulässigen Datenerhebung. Sie konkretisieren damit den Anwendungsbereich von § 7 Abs. 1 lit. c) KDG, mit der Folge, dass nur der dort jeweils wiedergegebene Datenkatalog zur rechtmäßigen Aufgabenerfüllung erforderlich ist.

- So ergibt sich für Schulen aus § 1 Abs. 1, 2 der Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft (SchulDO), welche Informationen über Schüler und Eltern gespeichert werden dürfen. Weitere Daten dürfen insoweit nur mit Einwilligung der betroffenen Person gespeichert werden (siehe: § 1 Abs. 3 SchulDO).
- Für Krankenhäuser ist der Umfang der Datenverarbeitung durch § 2 Abs. 1 der Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern (KrhDSO) geregelt und orientiert sich dabei an den standesrechtlichen Dokumentationspflichten und der Notwendigkeit zur Abrechnung der erbrachten Leistungen.
- Die Träger kirchlicher Friedhöfe haben in dieser Hinsicht § 1 Abs. 1 - 4 der Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft zu beachten.
- Für Kindertagesstätten im Bistum Hildesheim ist der Datenumfang bei der Anmeldung durch § 3 Abs. 2 und bei der Aufnahme zusätzlich durch § 5 Abs. 4 der Ordnung zur Regelung der Betreuungsverhältnisse in katholischen Tageseinrichtungen für Kinder festgelegt worden.

Eine Rechtsgrundlage besteht auch immer dann, wenn eine gesetzlich geregelte Mitteilungs- und Auskunftspflicht gegenüber öffentlichen Stellen besteht. Die Beschaffung der hierfür notwendigen Informationen ist stets erforderlich.
In allen anderen Fällen ist zunächst die Aufgabe, zu deren Unterstützung die Datenverarbeitung eingesetzt werden soll, klar zu definieren. Sodann ist zu fragen, welche Informationen nicht fehlen dürfen ohne dass die Aufgabenerfüllung gefährdet wäre. Hat eine Dienststelle beispielsweise die Aufgabe, Zahlungen an Dritte zu bewirken, so ist für die ordnungsgemäße Erstellung des Überweisungsträgers die Kenntnis des vollständigen Namens des Kontoinhabers, die Bezeichnung der kontoführenden Stelle, die IBAN-Nummer und die Höhe des Zahlungsbetrages erforderlich. Diese Daten dürfen also in diesem Zusammenhang erhoben werden, mehr nicht. Der Diözesandatenschutzbeauftragte kann die Einhaltung dieser Verpflichtung überwachen (§ 44 Abs. 1 KDG).

3. Sachliche Richtigkeit

Selbstverständlich müssen die verarbeiteten Daten aktuell und sachlich richtig sein. Anders kann eine ordnungsgemäße Verwaltung nicht erfolgen. Schreiben würden die betroffene Person nicht rechtzeitig erreichen, wenn die ermittelte Anschrift unrichtig ist. Schlimmer ist aber noch der Umstand, dass auch inhaltlich falsche Entscheidungen getroffen werden könnten, wenn unrichtige Informationen bestehen. Eigentlich braucht diese Anforderung nicht erwähnt zu werden. Trotzdem ist diese Verpflichtung in § 7 Abs. 1 lit. d) KDG ausdrücklich geregelt. Der Grund dafür ist, dass dieser Umstand vor allem in der elektronischen Datenverarbeitung keineswegs selbstverständlich ist. Zu oft werden Daten aus anderen Quellen übernommen, ohne dass überprüft wird, ob diese noch stimmen. Weitere Gefahr ist, dass mehrere Mitarbeiter den gleichen Datensatz ändern können und dies in unterschiedlicher Weise tun, weil ihr Informationstand differiert. Hier sollte festgelegt werden, wer zur Änderung des Datenbestandes berechtigt ist und dies sollte gleichzeitig durch bestimmte elektronische Bearbeitungsrechte abgesichert werden (Lese-, Änderungs-, Löschungsrecht). Dabei muss trotzdem auch gewährleistet sein, dass sachlich unrichtige Daten unverzüglich berichtigt oder gelöscht werden.

4. Bestandsschutz

In vielen Fällen ist die betroffene Person nicht nur auf die inhaltliche Richtigkeit ihrer Daten, sondern auch auf deren gesicherten Bestand angewiesen. Ihre Rechte hängen oft wesentlich davon ab, dass ihre Daten nicht verloren gehen oder gar zerstört werden. Bestes Beispiel hierfür ist eine elektronische Personalverwaltung. In § 7 Abs. 1 lit. f) KDG wird deshalb ausdrücklich gefordert, dass die Daten durch technische und organisatorische Maßnahmen vor unbefugtem Verlust, unbeabsichtigter Zerstörung oder Schädigung zu sichern sind. Hierfür sind insbesondere zwei Dinge von wesentlicher Bedeutung.

- Eine ausreichende Schulung der Mitarbeiter im Umgang mit der Anwendungssoftware.
- Eine ausreichende Datensicherung. Dabei ist zu berücksichtigen, ob diese nur hausintern oder auf einem externen Server erfolgt. Eine intern vorgenommene Speicherung kann durch Brand, Hochwasser und ähnliche Ereignisse zerstört werden. Oftmals sind dann im Wege der Datenrettung nur ein Teil der gespeicherten Datensätze wiederherstellbar. Wenn insoweit kein ausreichender Brand- oder Hochwasserschutz im eigenen Betrieb erfolgen kann, empfiehlt sich eine zusätzliche externe Sicherung.

Darüber hinaus muss auch die Funktionsfähigkeit der Wiederherstellung überprüft werden.

Die zunehmende Verbreitung von Erpressungsprogrammen (Ransomeware), bei denen der normale Datenbestand durch Vornahme externer Verschlüsselung für den Anwender gesperrt wird, hat auch gezeigt, wie wichtig eine kompetente Datensicherung auch nach außen hin sein kann. In manchen Fällen war es nicht möglich, die Blockade des eigenen Systems zu beseitigen, so dass hier nur die Möglichkeiten bestanden, entweder zu zahlen (was nicht immer zur Aufhebung der externen Verschlüsselung geführt hat) oder auf eine nicht von diesem System erfasste Datensicherung zurückzugreifen.

5. Sicherung vor unberechtigtem Zugang

Die gleiche Vorschrift, nämlich § 7 Abs. 1 lit. f) KDG verlangt auch, einen Schutz vor unbefugter oder unrechtmäßiger Datenverarbeitung sicherzustellen. Hierfür ist eine Reihe von organisatorischen und technischen Maßnahmen durchzuführen, die von allen Mitarbeitern unterstützt werden müssen. Dabei ist unter anderem folgendes zu beachten:

- Jeder Mitarbeiter, der personenbezogene Daten verarbeitet, muss sich mit einem individuellen Account am System anmelden. Der Anmeldevorgang besteht immer in der Angabe des für den Sachbearbeiter festgelegten Namens (Username) und eines Passwortes. Das Passwort kann von Hand eingegeben werden oder über einen Speicherstift und bei modernen Systemen auch durch Fingerabdruck oder Gesichtserkennung. Die letzteren Möglichkeiten haben zwar den Charme der Unvergesslichkeit, bieten dafür aber auch eine ganze Reihe von Risiken, die vorher ausgiebig geprüft werden müssen. Wie groß ist vor allem die Gefahr durch nachgemachte Fingerabrücke oder durch Bilder der Person sich unberechtigten Zugang zu verschaffen. Wo werden die Originaldateien der Abdrücke oder Aufnahmen gespeichert und sind sie für Dritte erreichbar?
- Jeder Mitarbeiter muss sich dabei auch eine Einschränkung seiner Rechte gefallen lassen. Das gilt sowohl für die Zurverfügungstellung der Anwendungssoftware, wie auch für den Umfang der Daten und die Möglichkeiten diese Daten zu bearbeiten (Lese-, Schreib-, Druck-, Kopier-, Versand- und Veränderungsrechte). Zu gewährleisten ist dabei, dass jeder Mitarbeiter nur die Datensätze bearbeiten kann, für die er auch fachlich zuständig ist.
- Der Schutz gegenüber Dritten muss durch Geheimhaltung des eigenen Passworts aufrechterhalten werden. Hierzu kann auch eine Änderung des Passworts notwendig

sein, wenn der Verdacht besteht, dass andere das aktuelle Kennwort erfahren haben könnten.

- Der Verzicht auf den Einsatz eigener und meist vom Dienstgeber nicht genehmigter Programme gehört ebenso dazu.
- Es hat sich auch zunehmend eingebürgert, sich dadurch unberechtigten Zugang zu verschaffen, indem Anhänge zu Mail-Schreiben versendet werden, die Zugangsberechtigungen ausspähen. Hierbei wird immer dreister gefälscht, so dass der Unterschied zu Originalschreiben immer schwerer zu erkennen ist. Daher ist ein sehr bewusster Umgang mit der Mail-Korrespondenz erforderlich. Vielfach kann man bei genügender Aufmerksamkeit doch noch erkennen, dass es sich um eine Späh-Mail handelt. Beispielsweise die Fragen, ob eine Nachricht von dieser Seite erwartet wird, ob der vermeintliche Absender sie überhaupt in dieser Form versenden würde, ob der richtige Empfänger angesprochen worden ist, können schon erhebliches Misstrauen erzeugen. In Zweifelsfällen sollten sie sich an ihre Geschäftsleitung und den Systemadministrator wenden um größeren Schaden zu verhindern.

Schaubild zur Rechtmäßigkeit und Ordnungsgemäßheit der Datenverarbeitung

Übersichtliche Zusammenfassung der Punkte aus Kapitel A und B

		Vorab zu klärende Fragen	Vorschriften des KDG
1.	**Rechtsgrundlage**		§ 6 Abs. 1
	A.	**Liegt eine Einwilligung der betroffenen Person vor?**	§ 6 Abs. 1 lit. b)
		• Schriftliche Erklärung. Besteht ein Muster hierfür? • Ist die Einwilligung nachweisbar? Dokumentation? • Wurde die Einwilligung freiwillig, informiert und bezogen auf den Einzelfall abgegeben?	§ 8 Abs. 1 – 5
		• Welche Möglichkeiten bestehen zum Widerruf der Einwilligung?	§ 8 Abs. 6
		• Liegt die Einwilligung der Sorgeberechtigten vor?	§ 8 Abs. 8
	B.	**Besteht ein gesetzlicher Erlaubnistatbestand?**	§ 6 Abs. 1 lit. a)
		• Liegt eine genaue Bezeichnung der anzuwendenden Rechtsvorschrift vor? • Sind die Zwecke der Verarbeitung genau festgelegt?	§ 6 Abs. 1 lit. c) bis g)
	C.	**Werden besondere Kategorien personenbezogener Daten verarbeitet?**	§ 11 Abs. 1
		Liegt eine der Ausnahmevorschriften hierzu vor?	§ 11 Abs. 2 lit. a) bis j)
	D.	**Durchbrechung der Zweckbindung**	§ 6 Abs. 2
		Liegt eine der Ausnahmevorschriften hierzu vor?	§ 6 Abs. 2 lit. a) bis j), Abs. 4, Abs. 6
2.	**Verarbeitungsgrundsätze**		§ 7 KDG
	A.	**Rechtmäßigkeit und Transparenz**	§ 7 Abs. 1 lit. a)
		Können die betroffene Person die Art und Weise der Datenverarbeitung nachvollziehen?	
	B.	**Einhaltung der Zweckbindung**	§ 7 Abs. 1 lit. b)
		Stehen Verfahren zur Anonymisierung und Pseudonymisierung zur Verfügung?	
	C.	**Datenminimierung**	§ 7 Abs. 1 lit. c)
		Beschränkt sich der Umfang der Datenverarbeitung auf das unbedingt erforderliche Maß?	
	D.	**Sachliche Richtigkeit / Aktualität**	§ 7 Abs. 1 lit. d)

		Wie wird eine Berichtigung der Daten organisatorisch sichergestellt?	
	E.	**Speicherbegrenzung**	§ 7 Abs. 1 lit. e)
		Werden personenbezogene Daten länger gespeichert, als es für die Zwecke ihrer Verarbeitung notwendig ist?	
	F.	**Angemessene Sicherheit**	§ 7 Abs. 1 lit. f)
		Durch welche Maßnahmen werden Integrität und Vertraulichkeit der Daten gesichert?	
	G.	**Nachweis der Einhaltung**	§ 7 Abs. 2
		Liegt eine Beschreibung des Verfahrens vor?	

III. Unmittelbare und mittelbare Datenerhebung

Wir haben in Kapitel A. und B. festgestellt, wann eine Datenverarbeitung zulässig ist und welche Verarbeitungsgrundsätze hierbei beachtet werden müssen. Dieses Kapitel beschäftigt sich mit der Frage, welche Möglichkeiten die Einrichtungen haben, die erforderlichen Daten zu erhalten. Grundsätzlich bestehen hierzu zwei Möglichkeiten. Die Erhebung der Daten bei der betroffenen Person, also die unmittelbare Datenerhebung sowie die Nutzung von Daten Dritter und die Informationsbeschaffung durch eigene Ermittlungen (unmittelbare Datenerhebung). Das KDG regelt die beiden Möglichkeiten jeweils in den Vorschriften der §§ 15,16 KDG. Im Hinblick auf das Ziel, der Wahrung des informationellen Selbstbestimmungsrechts der betroffenen Person, steht natürlich die unmittelbare Datenerhebung im Vordergrund.

1. Unmittelbare Datenerhebung

Für die unmittelbare Datenerhebung spricht auch eine Reihe von praktischen Vorteilen für die jeweiligen Einrichtungen.

- Die betroffene Person weiß, welche Daten über sie erhoben worden sind.
- Die Zwecke der Datenerhebung wurden ihr mitgeteilt, so dass Informationspflichten, wie sie in § 16 Abs. 1 und 2 KDG verlangt werden, entfallen.
- Die Verlässlichkeit der erhoben Daten ist größer. Niemand weiß in der Regel besser über sich Bescheid, als die betroffene Person selbst.
- Eine nach § 6 Abs. 1 lit. b) KDG notwendige Einwilligung kann unmittelbar und im Kontext mit der Person eingeholt werden.

- Eine faire und transparente Verarbeitung der Daten ist durch Information der betroffenen Person über seine gesetzliche Verpflichtung zur Bereitstellung der Daten, die Möglichkeit des Widerrufs einer erteilten Einwilligung, die Dauer der Speicherung, seine Rechte auf Auskunft sowie die Änderung, Sperrung oder Löschung der Daten zu erreichen, leichter möglich.
- Die betroffene Person kann auf die Tätigkeit des betrieblichen Datenschutzbeauftragten und auf die Möglichkeit einer Beschwerde an den Diözesandatenschutzbeauftragten hingewiesen werden.
- Wird von diesen Möglichkeiten Gebrauch gemacht, dürfte dieses zur Stärkung des Vertrauensverhältnisses zwischen den Beteiligten führen.

Gegen eine unmittelbare Datenerhebung spricht nur

- deren faktische Unmöglichkeit, wie sie zum Beispiel auf gleichartige Datenverarbeitungen, die in großer Zahl vorgenommen werden, zutrifft (Beispiel: Meldewesen);
- sie gesetzlich anders geregelt ist;
- ein Anlass besteht, die Angaben der betroffenen Person zu überprüfen;
- wenn die betroffene Person trotz Aufklärung Angaben verweigert, zu denen er gesetzlich verpflichtet ist.
- oder einer der Gründe aus § 15 Abs. 5 lit. a) bis c) vorliegt.

Die unmittelbare Erhebung erfolgt in der Regel durch die Verwendung von Fragebögen, Aufnahmeverträgen, Personalbögen und anderen Formularen, die von der betroffenen Person jeweils selbst ausgefüllt werden. In der heutigen Zeit ist jedoch auch eine direkte Eingabe der Informationen in das Datenverarbeitungssystem der Dienststelle in Anwesenheit der betroffenen Person möglich. Hierbei muss jedoch immer für den Einzelnen erkennbar bleiben, für welchen Zweck seine Daten benötigt und gespeichert werden. Notfalls ist dies von der aufnehmenden Person zu erläutern. In beiden Fällen sind ihm auch die Informationen nach § 15 Abs. 1 und 2 KDG zu übermitteln. Diese können auch in einen Erläuterungsteil des Formulars eingebunden werden.

Sollte sich herausstellen, dass die Informationen noch für einen anderen Zweck benötigt werden, als er bei der Datenerhebung angegeben worden ist, so ist die betroffene Person nach § 15 Abs. 3 KDG vor dieser Weiterverarbeitung über die Änderung des Verarbeitungszweckes und die hierfür maßgeblichen Gründe zu unterrichten. Ihm wird hiermit die Möglichkeit gegeben, sich zu wehren und der anderweitigen Nutzung zu wiedersprechen.

Was wird von mir erwartet?

- Eine Datenerhebung bei der betroffenen Person selbst durchzuführen, solange keine Ausnahmegründe vorliegen.
- Der betroffenen Person dabei die Informationen zu erteilen, die in § 15 Abs. 1 und Abs. 2 KDG benannt sind.
- Ihn über eine Änderung des Nutzungszwecks nach § 15 Abs. 3 KDG vorab zu informieren.

2. Mittelbare Datenerhebung

Eine mittelbare Datenerhebung, ohne die Mitwirkung der betroffenen Person sollte nur in den Fällen durchgeführt werden, die zuvor in der Liste aufgezählt wurden. Dabei sind die Regeln aus § 16 KDG zu beachten.

- Über die schon zuvor genannten Informationen nach § 15 Abs. 1, 2 KDG hinaus, ist die betroffene Person über die erhobenen Daten und die Quelle aus der sie stammen zu unterrichten (Abs. 1).
- Bei diesen Informationen müssen zudem die Hinweise nach Abs. 2 erfolgen. Wichtig ist hierbei besonders, dass die Notwendigkeit der Verarbeitung dieser Daten der betroffenen Person innerhalb einer angemessenen Frist, spätestens aber nach einem Monat erläutert werden muss.
- Bei einer Beabsichtigung der Weiterverarbeitung zu einem anderen Zweck, als den für die sie erhoben worden sind, muss die betroffene Person auch hier ebenfalls über die weitere Verwendung und deren maßgebliche Gründe vorher unterrichtet werden (Abs. 3).

Hiervon kann nur in den Fällen der Absätze 4 und 5 abgewichen werden. In diesen Fällen hat der Verantwortliche nach Absatz 6 geeignete Maßnahmen zum Schutz der betroffenen Person zu ergreifen und die Gründe für das Absehen der Information schriftlich festzuhalten.

IV. Offenlegung personenbezogener Daten

Der Begriff „Offenlegung“ hat die früher verwendete Bezeichnung „Datenübermittlung“ abgelöst. Eine inhaltliche Änderung gegenüber dem alten Recht nach der KDO ist nicht erfolgt. Zu

unterscheiden ist die Offenlegung gegenüber kirchlichen und öffentlichen Stellen (§ 9 KDG) von der Offenlegung gegenüber nicht kirchlichen und nicht öffentlichen Stellen (§ 10 KDG).

1. Offenlegung gegenüber kirchlichen Stellen

Kirchliche Stellen sind alle Dienststellen und Einrichtungen, die in § 3 Abs. 1 lit. a) bis c) KDG aufgeführt sind. Einrichtungen, die zwar kirchlich geprägt sind aber nicht an der Verwirklichung der drei Grunddienste kraft bischöflichen Auftrags teilhaben, fallen nicht hierunter. Als Beispiel mögen hier katholische Studentenverbindungen dienen.

Eine Weitergabe personenbezogener Daten an andere Einrichtungen ist immer eine Gefahr für das informationelle Selbstbestimmungsrecht des Einzelnen. Dieser soll ja auch erkennen können wer, was und bei welcher Gelegenheit über ihn weiß. Deshalb ist eine Offenlegung nur unter bestimmten Voraussetzungen zulässig.

- Die Kenntnis der übermittelten Daten muss für die empfangende Stelle aus dienstlichen Gründen erforderlich sein (Abs. 1 lit. a)).
- Die Offenlegung muss zu dem gleichen Zweck erfolgen, für den die Daten erhoben worden sind. Trifft diese Voraussetzung nicht zu, kann sie ausnahmsweise trotzdem erfolgen, wenn eine der Voraussetzungen des § 6 Abs. 2 KDG gegeben ist (Abs. 1 lit. b)).
- Die empfangende Stelle darf die Daten nur für den Zweck verarbeiten, für den sie ihr übermittelt worden sind (Abs. 4). Zulässig ist eine Verarbeitung für andere Zwecke nur dann, wenn auch hier die Voraussetzungen aus § 6 Abs. 2 KDG vorliegen.
- Sind Daten die offengelegt werden dürfen mit anderen personenbezogenen Daten der gleichen oder einer anderen Person verbunden, so dass sie nicht getrennt werden können, können auch sie offengelegt werden. Voraussetzung ist allerdings, dass berechtigte Interessen der betroffenen Person an der Geheimhaltung nicht offensichtlich überwiegen (Abs. 6). In diesem Fall hat die Offenlegung gänzlich zu unterbleiben. Eine Verarbeitung dieser zusätzlichen Daten durch die empfangende Stelle ist in jedem Fall unzulässig.
- Die Verantwortung für die Zulässigkeit der Offenlegung trägt die abgebende Stelle (Abs. 3 Satz 1). Bei einer Offenlegung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung (Abs. 3 Satz 2). Allerdings muss die abgebende Stelle auch in diesem Fall überprüfen, ob das Offenbarungsersuchen im Rahmen der dienstlichen Aufgaben des Empfängers liegt (Abs. 3 Satz 3).

Bei einer Offenlegung auf Ersuchen der empfangenden Stelle muss diese Verfahrensweise unter Berücksichtigung der schutzwürdigen Interessen der Person und den Aufgaben oder Geschäftszwecken der beteiligten kirchlichen Stellen angemessen sein (Absatz 2). Vorzunehmen ist hier also eine Güterabwägung zwischen Individualinteresse und berechtigter Aufgabenerfüllung. Der Absatz 2 bildet insoweit die einzig neue Vorschrift in diesem Bereich.

2. Offenlegung gegenüber öffentlichen Stellen

Umfasst werden hier alle öffentlichen Stellen, die nicht zur Kirche im Sinne von § 3 Abs. 1 KDG gehören. Für sie gelten die gleichen Regelungen, wie für kirchliche Stellen, jedoch ergänzt durch die Verpflichtung, dass auch sie ausreichende Datenschutzmaßnahmen getroffen haben müssen.

Für staatliche Behörden der Kommunen, der Länder oder des Bundes, die zur Anwendung der Datenschutzgrundverordnung verpflichtet sind und der Aufsicht staatlicher Kontrollbehörden unterstehen, kann dies ohne weiteres angenommen werden.

Das gleiche gilt für öffentliche Stellen der Evangelischen Kirchen, die jeweils das Datenschutzgesetz der EKD (DSG-EKD) zu beachten haben und der Aufsicht des Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland oder des Datenschutzbeauftragten für die Evangelische Kirche in Norddeutschland unterstehen.

3. Offenlegung gegenüber nicht kirchlichen und nicht öffentlichen Stellen

Bei der Offenlegung gegenüber nicht kirchlichen und nicht öffentlichen Stellen sind zwei Fälle zu unterscheiden.

1. Die Offenlegung ist zur Erfüllung dienstlicher Aufgaben der offenlegenden kirchlichen Stelle erforderlich (§ 10 Abs. 1 lit. a) KDG) und die Voraussetzungen nach § 6 KDG vorliegen.
2. Die Offenlegung erfolgt auf Ersuchen des Empfängers, der ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegt und kein schutzwürdiges Interesse der betroffenen Person am Ausschluss der Offenlegung besteht.

Die Verantwortung für die Zulässigkeit der Offenlegung trägt in beiden Fällen die offenlegende Stelle (§ 10 Abs. 2 KDG). Die betroffene Person ist in der Regel über die Offenlegung

ihrer Daten zu unterrichten (§ 10 Abs. 3 Satz 1). Das gilt jedoch nicht, wenn sie schon auf andere Weise hiervon Kenntnis erlangt hat oder eine Güterabwägung ergibt, dass die Vermeidung einer Gefahr für die öffentliche Sicherheit oder des kirchlichen Wohls Vorrang vor den schutzwürdigen Interessen der betroffenen Person hat (§ 10 Abs. 3 Satz 2).

Die Empfänger dürfen in beiden Fällen die Daten nur für den Zweck verarbeiten, für den sie übermittelt worden sind (§ 10 Abs. 4 KDG). Hierauf hat ihn die offenlegende Stelle ausdrücklich hinzuweisen. Eine Weiterverarbeitung für andere Zwecke ist nur zulässig, wenn eine der Ausnahmen nach § 6 Abs. 2 vorliegen und die offenlegende Stelle zugestimmt hat (§ 10 Abs. 4 Satz 3 KDG).

V. Informationspflichten gegenüber den betroffenen Personen

1. Grundsatz der Transparenz

Eine sehr wichtige Neuerung des KDG ist die Aufnahme des Grundsatzes der Transparenz durch die Bestimmung in § 14. Sie etabliert auch für das kirchliche Recht den Grundsatz, dass die Information und Kommunikation mit den betroffenen Personen, deren Daten verarbeitet werden in offener, eben transparenter Form stattzufinden hat. Das gilt für alle Schritte, die in der Datenverarbeitung gemeinsam mit der betroffenen Person verwirklicht werden. Angefangen von der Datenerhebung (§§ 15, 16 KDG) über die Geltendmachung der Rechte der betroffenen Personen (§§ 17 bis 25) bis hin zur Benachrichtigung über eine fehlerhafte Verarbeitung, soweit sie ein hohes Risiko für die persönlichen Rechte der betroffenen Person darstellt (§ 34).

Was wird unter einer transparenten Information der betroffenen Personen verstanden? Nach dem Text der Vorschrift muss diese:

- In leicht zugänglicher Form erreichbar sein.
- Präzise über Art der Datenverarbeitung unterrichten.
- Für die betroffene Person verständlich sein, insbesondere dann, wenn es sich dabei um noch minderjährige Personen handelt.

An die Verständlichkeit werden hohe Anforderungen gestellt. Sie liegt nur dann vor, wenn eine klare und einfache Sprache benutzt wird, die für jedermann ohne weiteres verständlich ist. Juristisch formulierte Texte wie „Allgemeine Geschäftsbedingungen“ oder ähnliche scheiden daher aus. Auch die Verwendung einer Fachterminologie mit fremdsprachlichen und

nicht allen Personen verständlichen Begriffen dürfte der Forderung nicht gerecht werden. Zur Erleichterung können auch standardisierte Bildsymbole eingesetzt werden, weil solche heute schneller verstanden werden, als entsprechend lange Erklärungen. Bei Menschen mit Migrationshintergrund muss zudem die Frage gestellt werden, ob die Informationen nicht auch in der ihnen vertrauten Heimatsprache anzubieten sind.

Die Informationen sind schriftlich, gegebenenfalls auch elektronisch bereitzuhalten. Das zur Verfügung stellen in elektronischer Form dürfte sich vor allem bei Internetdiensten anbieten. Nur wenn von der Person verlangt, kann die Information auch mündlich erteilt werden. Diese Ausnahme soll auch Personen mit Leseschwäche gerecht werden.

Die bei der Datenerhebung zu erteilenden Informationen nach § 15 Abs. 1 bis 3 und § 16 Abs. 1 bis 3 können daher durch einen Vordruck erteilt werden, der diesen Anforderungen entspricht. Die ebenfalls geforderte Präzision der Unterrichtung wird hier durch vollständige Berücksichtigung der gesetzlich festgelegten Angaben erreicht.

2. Transparenz bei Ausübung der Rechte durch die betroffene Person

Hat die betroffene Person Einwände gegen den Umfang der Datenerhebung oder die Art und Weise ihrer Verarbeitung, hat sie die Möglichkeit ihre Rechte nach § 17 bis 25 KDG geltend zu machen. Damit ihr dies ohne Schwierigkeiten möglich ist, braucht sie aber oft die Unterstützung durch die verarbeitende Stelle. Daher verpflichtet § 14 Abs. 2 die Verantwortlichen, der betroffenen Person die Wahrnehmung ihrer Rechte zu erleichtern. Welche Wege sind hierbei angemessen? In der Regel wird hier zumindest Folgendes notwendig sein:

- Seine Einwände werden mit ihm sachlich erörtert.
- Hierbei wird er in angemessener Form über die bestehende Rechtslage informiert.
- Dabei wird auch in verständlicher Weise dargelegt, aus welchen Gründen die Daten von ihm erhoben werden, wozu man sie benötigt und an welche Stellen sie weitergeleitet werden können.
- Im Bedarfsfall wird ihm auch dargelegt, wie seine Daten vor unberechtigtem Zugriff gesichert sind.
- Die betroffene Person wird über seine hierzu bestehenden Rechte unterrichtet.
- Ihm werden die Stellen genannt, an die er sich wenden kann.

Das alles wird in einer freundlichen Atmosphäre vorgenommen, die deutlich macht, dass man selbstverständlich bereit ist, seine berechtigten Interessen zu wahren.

Sind auf Grund dieses Gesprächs oder durch das Eingreifen der Aufsichtsbehörde Maßnahmen nach § 17 – 25 KDG durchzuführen, so hat dies unverzüglich zu geschehen, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags (§ 14 Abs. 3 Satz 1). Zur Transparenz gehört in diesem Falle auch, dass die betroffene Person auch über Schwierigkeiten bei der Umsetzung, die eine Fristverlängerung erforderlich macht (§ 14 Abs. 3 Satz 2 und 3) oder bei Untätigkeit (§14 Abs. 4) über die Gründe informiert wird.

3. Informationspflicht bei der Datenerhebung

Der Informationspflicht bei der Erhebung personenbezogener Daten hat das Gesetz über den kirchlichen Datenschutz besondere Bedeutung zuerkannt und sie in zwei umfangreichen Vorschriften der §§ 15 und 16 ausführlich geregelt. Der Grund dafür liegt darin, dass die Einschränkung und Beeinträchtigung des informationellen Selbstbestimmungsrechts mit der Datenerhebung beginnt. Dabei wird es für die betroffene Person wichtig sein zu erfahren, warum gerade diese Daten von ihm gebraucht werden, auf welcher Rechtsgrundlage dies erfolgt, für welche Zwecke sie verarbeitet werden sollen, welche weiteren Stellen diese Daten ebenfalls erhalten und ob sie ausreichend geschützt sind.

Diesem Anspruch wird das KDG mit Festlegung der notwendigen Informationen in § 15 Abs. 1 bis 3 für die unmittelbare Datenerhebung und § 16 Abs. 1 bis 3 für die mittelbare Datenerhebung gerecht. Die Liste der mitzuteilenden Punkte ist verbindlich. Das ergibt sich unmittelbar aus dem Wortlaut der Bestimmungen. Formulierungen, wie „teilt … mit“ oder „stellt … zur Verfügung“ lassen keinen Spielraum offen. An keiner Stelle ist hier eine „Kann-Bestimmung“ verwendet worden. Fairness und Transparenz müssen gerade auch in der ersten Phase der Datenverarbeitung von Anfang an gewährleistet werden (siehe § 15 Abs. 2).

Bei mittelbarer Datenerhebung (§ 16) kommt zu den Informationspflichten nach § 15 Abs. 1 und 2 noch hinzu, dass die betroffene Person über die erhobenen Daten unterrichtet werden muss, die sie sonst mangels eigener Angaben nicht kennen muss und auf ihre Richtigkeit überprüfen könnte. Darüber hinaus ist sie über die Quelle der Herkunft zu unterrichten (§ 16 Abs. 1 lit. a) und b)). Der Absatz 2 verlangt, dass diese Information in angemessener Frist, spätestens jedoch nach einem Monat zu erfolgen hat. Zu berücksichtigen ist hierbei, dass die betroffene Person anders als in der Situation der unmittelbaren Datenerhebung nicht sofort über den Umfang und Inhalt der Daten informiert wird. Bei einer Datenerhebung ohne ihre Beteiligung besteht keine Veranlassung, ihr diese Information lange vorzuenthalten. In „angemessener Frist“ kann daher nur so verstanden werden, dass die betroffene Person im

Rahmen der organisatorischen Leistungsfähigkeit des Datenverarbeiters nach Möglichkeit sofort unterrichtet wird. Bei einer weiteren Datenerhebung, bei der die Angaben, welche die betroffene Person unmittelbar angegeben hat, nun noch durch weitere Informationen einer dritten Stelle ergänzt werden sollen, kann es auch angemessen sein, ihn beim demnächst stattfindenden persönlichen Treffen über die erhaltenen Daten zu informieren.

Die gleichen Überlegungen sind in den Fällen von § 16 Abs. 2 lit. b) und c) zu treffen, die den Informationszeitpunkt spätestens auf den Zeitpunkt der ersten Mitteilung oder den der erstmaligen Offenlegung festlegen.

Die Informationen sind nach § 14 Abs. 5 der betroffenen Person kostenlos zur Verfügung zu stellen. Ausnahmen hiervon bestehen nur für den Fall querulatorischer Anfragen. Sie sind dann gegeben, wenn sie offenkundig unbegründet sind oder durch ausufernde, häufige Anfragen den Eindruck erwecken, dass die verarbeitende Stelle lediglich in ihrer Funktionsfähigkeit beeinträchtigt werden soll. Der Nachweis für das Vorliegen dieser Ausnahmen ist vom Verantwortlichen zu führen.

4. Auskunftsrecht der betroffenen Person

Ein weiteres wichtiges Auskunftsrecht der betroffenen Person ist in § 17 KDG geregelt. Es besteht während des gesamten Verarbeitungsvorgangs. Es ist nach § 25 Abs. 1 KDG unabdingbar, kann also nicht durch ein Rechtsgeschäft ausgeschlossen werden. Es gibt der betroffenen Person jederzeit die Möglichkeit, den Umfang personenbezogener Daten, ihre inhaltliche Richtigkeit, den Zweck ihrer Verarbeitung und eine mögliche Offenbarung Dritten gegenüber zu prüfen und gegebenenfalls sich hiergegen zur Wehr zu setzen.

Der § 17 Abs. 1 enthält unter lit. a) - h) einen Katalog von Informationen, die auf Anforderung der betroffenen Person in jedem Fall zu übermitteln sind. Dabei handelt es sich gewissermaßen um die „Essentialia“ des informationellen Selbstbestimmungsrechts. Die betroffene Person muss erkennen können wer (lit. c)) – was (lit. b)) – wann (lit. d)) – und bei welcher Gelegenheit (lit. a)) über ihn weiß. Auch die Informationen über bestehende Rechte und ihre Geltendmachung gehören dazu. Die Auskunft hierüber ist eine Pflichtangabe, die ebenfalls nach § 14 Abs. 5 KDG unentgeltlich vorzunehmen ist.

Besonderheiten bestehen bei der Übermittlung seiner personenbezogenen Daten in ein Drittland. Nach § 17 Abs. 2 KDG muss die betroffene Person auch über die nach § 40 KDG geeigneten Garantien informiert werden. Ausführliche Angaben hierzu können der KDG-

Praxishilfe 08 zur „Datenübermittlung in Drittländer“ der Konferenz der Diözesandatenschutzbeauftragten entnommen werden.

Gegenüber einem kirchlichen Archiv besteht der Auskunftsanspruch nur für den Fall, dass das Auffinden des Archivguts mit vertretbarem Aufwand ermöglicht werden kann.

Bei der Form der Auskunftserteilung ist § 17 Abs. 3 KDG zu berücksichtigen. Danach sind in der Regel Kopien zur Verfügung zu stellen (Satz 1). Der Ausdruck des Datenbestandes aus einem Anwendungsprogramm der elektronischen Datenverarbeitung ist als Kopie der dort gespeicherten Daten anzusehen, wenn das Erscheinungsbild bei der Darstellung der Daten nicht geändert wird. Wird das Auskunftsersuchen elektronisch gestellt, so ist auch die Zurverfügungstellung in einem elektronischen Format statthaft (Satz 3).

Die Folgen der Auskunftserteilung können in der Geltendmachung weiterer Rechte bestehen. Hier kommt insbesondere das Recht auf Berichtigung (§ 18 KDG), das Recht auf Löschung (§ 19 KDG), das Recht auf Einschränkung der Verarbeitung (§ 20 KDG) und das Widerspruchsrecht (§ 23 KDG) in Betracht.

VI. Die Rechte der betroffenen Person

1. Grundlagen

Die beste Kontrolle, so heißt es, geht immer von der betroffenen Person selbst aus. Deshalb muss sich jede Einrichtung bei ihrer Tätigkeit auch von ihm in Frage stellen lassen. Er hat das Recht die Verarbeitung seiner personenbezogenen Daten als nicht rechtmäßig, nicht notwendig, nicht zweckgebunden, fehlerhaft oder unvollständig zu beanstanden und somit auch eine auf ihn bezogene Kontrolle zu veranlassen. Hierzu sind ihm eine Reihe wichtiger Rechte eingeräumt:

1. Er kann erwarten, dass seine Daten nur auf einer Rechtsgrundlage oder mit seiner Einwilligung erhoben, gespeichert und verarbeitet werden.
2. Er kann erwarten, dass die Verarbeitung besonderer Kategorien seiner personenbezogenen Daten unterbleibt oder nur in den erlaubten Fällen verarbeitet werden.
3. Er kann verlangen, dass ihm Auskunft über die zu seiner Person gespeicherten Daten erteilt wird (Prinzip der Offenheit und Transparenz).
4. Er kann erwarten, dass seine Daten nur für die Zwecke genutzt werden, für die sie auch erhoben worden sind.

5. Er kann erwarten, dass seine Daten inhaltlich richtig und vollständig sind und im gegeben Fall berichtigt werden.
6. Er kann erwarten, nicht zum Objekt einer automatisierten Entscheidung gemacht zu werden.
7. Er hat das Recht zu verlangen, dass eine Einschränkung der Datenverarbeitung erfolgt, wenn deren Richtigkeit bestritten ist, gesperrt und nicht mehr genutzt werden.
8. Er kann erwarten, dass er unterrichtet wird, wenn ein Fehler der Datenverarbeitung zu einer Gefährdung seiner Rechte führen könnte.
9. Darüber hinaus hat er das Recht, sich gegen eine unberechtigte Datenverarbeitung zu wehren und zu verlangen, dass sie eingestellt wird.
10. Er kann verlangen, dass unzulässig gespeicherte oder nicht mehr benötigte Daten gelöscht werden.
11. Er kann erwarten, dass auch im Falle der Offenlegung seiner Daten, diese auch von den Empfängern gelöscht werden (sogenanntes „Right to be left alone“).
12. Schließlich hat er auch ein Recht auf Datenübertragung, wenn er die Verarbeitung seiner auf eine andere verantwortliche Person übertragen will.

Eine umfangreiche Liste hierzu ist nachfolgend unter Ziffer 2 beigefügt. Die Gewährleistung dieser Rechte ist von den datenverarbeitenden Stellen selbst vorzunehmen. Im Streitfall kann sich die betroffene Person an den zuständigen Datenschutzbeauftragten wenden. Auch die Dienststelle hat die Möglichkeit, sich an den Datenschutzbeauftragten zu wenden, wenn Unklarheit über ihre Verpflichtungen besteht.

Für jede kirchliche Verwaltung sind daher Antworten auf folgende Fragen zu finden:

- Werden die betroffenen Personen jeweils über die erhobenen Daten und die Art der Datenverarbeitung in transparenter Form unterrichtet? Sind die Informationen hierzu leicht zugänglich, präzise und leicht verständlich?
- Wie wird der betroffenen Person die Geltendmachung ihrer Rechte erleichtert. Wird sie hierbei über die ergriffenen Maßnahmen unverzüglich, spätestens aber innerhalb eines Monats unterrichtet?
- Gibt es dafür ein geregeltes Beschwerdeverfahren, das die betroffene Personen über die zuständige Stelle informiert und darüber, wo sie erreicht werden kann?
- Besteht eine Offenheit gegenüber Beschwerden? Werden die betroffenen Personen mit ihren Problemen, Fragen und Anregungen ernst genommen oder eher nach dem Motto behandelt „Wer sich beschwert, ist hier nicht willkommen!“.

- Welche Mitarbeiter sind für die Auskunftserteilung an die betroffenen Personen zuständig? Macht das jeder Mitarbeiter, der die Sache bearbeitet oder eine zentrale Stelle?
- Wie wird mit den Auskunftswünschen umgegangen? Erhält die betroffene Person Fotokopien der über ihn gespeicherten Daten, kann er den Datensatz auch in einem elektronischen Format erhalten?

Folgendes ist dabei zu bedenken: Auch eine rechtmäßige Datenverarbeitung greift in das grundrechtlich geschützte Recht der betroffenen Person auf informationelle Selbstbestimmung ein. Deshalb sollte jeder, der geltend machen will, dass datenschutzrechtliche Vorschriften nicht eingehalten worden sind, mit großem Respekt behandelt werden!

Genauere Auskünfte zu diesem Themenkomplex entnehmen Sie bitte der KDG-Praxishilfe 6 über „Betroffenenrechte“ der Konferenz der Diözesandatenschutzbeauftragten, die hier aus Vereinfachungsgründen nicht vollständig wiedergeben werden kann.

2. Übersicht über die Rechte der betroffenen Personen

Gesetzlich geregelte Rechte		**Regelungen im KDG**
Transparente Information	über die Datenerhebung, ihm zustehen-de Rechte und Benachrichtigung von Daten-schutzverletzungen	§ 14 Abs. 1
	in einer klaren und einfachen Sprache	§ 14 Abs. 1
	in schriftlicher oder elektronischer Form	§ 14 Abs. 1
	innerhalb einer angemessenen Frist	§ 14 Abs. 1
Anspruch auf Erleichterung	der Geltendmachung eigener Rechte	§ 14 Abs. 2
	durch Information über getroffene Maßnahmen	§ 14 Abs. 3
	innerhalb 1 Monats	
Unentgeltlichkeit der Informationen	über die Datenerhebung sowie erteilte Aus-künfte im Rahmen der Rechtswahrnehmung durch die betroffene Person	§ 14 Abs. 5
Informationsanspruch	bei unmittelbarer Datenerhebung	§ 15 Abs. 1, 2
	bei mittelbarer Datenerhebung	§ 16 Abs. 1 bis 3
Auskunftsrecht	Umfang der Auskunft	§ 17 Abs. 1
	Form der Auskunft	§ 17 Abs. 3
	(Kopien, elektronisches Format)	
	Bei Übermittlung in ein Drittland	§§ 17 Abs. 2, 40
Berichtigung	unrichtiger Daten	§ 18 Abs. 1 Satz 1
Vervollständigung	unvollständiger Daten	§ 18 Abs. 1 Satz 2
Löschung	nicht mehr notwendiger Daten	§ 19 Abs. 1 lit. a)
	bei Widerruf der Einwilligung	§ 19 Abs. 1 lit. b)
	bei Widerspruch gegen die Verarbeitung	§ 19 Abs. 1 lit. c)
	bei unrechtmäßiger Verarbeitung	§ 19 Abs. 1 lit. d)
	zur Erfüllung einer rechtl. Verpflichtung	§ 19 Abs. 1 lit. e)
Löschung öffentlicher Daten	durch Mitteilungen an die Datenempfänger, die Löschung ebenfalls durchzuführen	§ 19 Abs. 2
Einschränkung der Verarbeitung	bei Bestreiten der Richtigkeit der Daten	§ 20 Abs. 1 lit. a)
	bei unrechtmäßiger Verarbeitung	§ 20 Abs. 1 lit. b)
	bei nicht mehr benötigten Daten	§ 20 Abs. 1 lit. c)
	bei Widerspruch gegen die Verarbeitung	§ 20 Abs. 1 lit d)
Datenübertragung	durch Verfügbarmachung in einem maschinen-lesbaren Format	§ 22 Abs. 1 Satz 1
	und Weitergabe an einen anderen Verantwort-lichen	§ 22 Abs. 1 Satz 2
	alternativ: durch direkte Übermittlung an den	§ 22 Abs. 2

	anderen Verantwortlichen	
Widerspruchsrecht	gegen eine Verarbeitung nach § 6 Abs. 1 lit. f) oder g) gegen eine Verarbeitung bei Direktwerbung oder Fundraising durch Schaffung einer „Robinsonliste“	§ 23 Abs. 1 § 23 Abs. 2 § 23 Abs. 3
Vermeidung rein automatisierter Entscheidungen	die rechtliche Wirkung entfalten oder in ähnlicher Weise beeinträchtigen	§ 24 Abs. 1
Unabdingbare Rechte	Die nicht durch Rechtsgeschäft ausgeschlossen werden können (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch)	§ 25

Hinweis in eigener Sache

Der Inhalt dieser Arbeitshilfe wurde mit größter Sorgfalt erstellt und erhebt keinen Anspruch auf Vollständigkeit.

Diese Arbeitshilfe dient in erster Linie dazu, Ihnen bei der täglichen Arbeit die Einbindung der datenschutzrechtlichen Bestimmungen zu erleichtern. Sie berücksichtigt die Vorschriften des KDG durch den Diözesandatenschutzbeauftragten zum derzeitigen Zeitpunkt.

Sollten sich Unklarheiten oder offensichtliche Fehler aus dieser Arbeitshilfe ergeben, so bitten wir um einen entsprechenden Hinweis unmittelbar an den Diözesandatenschutzbeauftragten. Die Kontaktinformationen können Sie dieser Arbeitshilfe entnehmen.