Arbeitshilfe

Fortgeltung der KDO-DVO unter dem KDG

Auslegung der Datenschutzaufsichten

Stand 10/2018

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Arbeitshilfe

Fortgeltung der KDO-DVO unter dem KDG
- Auslegung der Datenschutzaufsichten -

Herausgegeben von der
Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands

So erreichen Sie uns:

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22

E-Mail: DDSB@kdsz.de
www.katholisches-datenschutzzentrum.de

Diese Arbeitshilfe der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands dient als Orientierung, welche Regelungen der KDO-DVO nach Auffassung der Diözesandatenschutzbeauftragten nach Inkrafttreten des KDG noch anwendbar sind und den Regelungen des KDG nicht entgegenstehen (vgl. § 57 Abs. 5 KDG). Sie stellt die gegenwärtige Interpretation durch die Diözesandatenschutzbeauftragten dar.

Revision 1.0 / 26.10.2018

Hinweise zu den nachfolgenden Ausführungen

Da es bei der Überarbeitung der Anordnung über den Kirchlichen Datenschutz (KDO) nicht möglich war, gleichzeitig auch die Durchführungsverordnung zur KDO (KDO-DVO) zu überarbeiten, findet sich in § 57 Abs. 5 des Gesetzes über den Kirchlichen Datenschutz (KDG) eine Übergangsregelung für die KDO-DVO.

Gemäß dieser Übergangsregelung sind die Vorgaben der KDO-DVO auch nach Inkrafttreten des KDG zu beachten, soweit sie den Regelungen des KDG nicht entgegenstehen. Die Übergangsphase gilt bis zum Inkrafttreten einer neuen Durchführungsverordnung, längstens aber bis zum 30.06.2019.

Auf Grund vielfacher Nachfragen zur Weitergeltung einzelner Regelungen der KDO-DVO haben die Datenschutzaufsichten der Katholischen Kirche mit dieser Arbeitshilfe ihre Anmerkungen zur Weitergeltung der KDO-DVO unter dem KDG zusammengestellt.

Diese Asführungen sind Auslegungshinweise der Datenschutzaufsichten. Die Hinweise sind insofern nicht verbindliche gesetzliche Vorgaben, bilden für die Bearbeitung von Einzelfällen oder die Beantwortung von Anfragen bei den Datenschutzaufsichten aber die Grundlage für deren Arbeit.

Für die folgenden Ausführungen wurde die Fassung der KDO-DVO des Erzbistums Paderborn verwendet. Bitte vergleichen Sie die Ausführungen mit der für Ihr (Erz-)Bistum geltenden Fassung der KDO-DVO.

Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz für das Erzbistum Paderborn

(KDO-Durchführungsverordnung – KDO-DVO)

Verwaltungsverordnung vom 13. Oktober 2015
(Erzbistum Paderborn KA 2015, Stück 10, Nr. 135)
- nichtamtliche Lesefassung -

I.
KDO-DVO

Aufgrund des § 22 der Anordnung über den kirchlichen Datenschutz für das Erzbistum Paderborn (KDO) vom 8. September 2003 (KA 2003, Nr. 194), zuletzt geändert durch 3. KDO-ÄndG vom 3. Dezember 2014 (KA 2014, Nr. 165), werden die folgenden Regelungen getroffen:

Inhaltsübersicht

KDO-DVO

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

(1) Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind diese vor Inbetriebnahme schriftlich dem Diözesandatenschutzbeauftragten zu melden. Sofern ein betrieblicher Datenschutzbeauftragter bestellt ist, ist diesem gemäß § 21 Abs. 2 KDO eine Übersicht nach § 3a Abs. 2 KDO zur Verfügung zu stellen.

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

II. Zu § 4 KDO:

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

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

(2) Über die Beachtung der Verpflichtung ist von den bei der Datenverarbeitung tätigen Personen eine schriftliche Erklärung nach näherer Maßgabe des Abschnittes

Anmerkung zur Weitergeltung

Neu: § 31 KDG

Es gelten die in § 31 KDG genannten Voraussetzungen für das „Verzeichnis von Verarbeitungstätigkeiten“.

Die Verpflichtung zur Vorlage vor Inbetriebnahme bei dem Diözesandatenschutzbeauftragten (DDSB) besteht nur noch auf Nachfrage des DDSB (§ 31 Absatz 4 KDG). Dem betrieblichen Datenschutzbeauftagten (bDSB) ist das Verzeichnis vorzulegen.

Diese Pflicht trifft (vertraglich) auch den Auftragsverarbeiter.
Die bisher verwendeten Muster, die mit Verweisen auf die bisherige Rechtslage entwickelt worden sind, können nicht mehr verwendet werden. (Allenfalls ist eine Nutzung der Muster nur für den internen Gebrauch denkbar).

Neu: § 5 KDG

Für die Verpflichtungserklärungen haben die Diözesandatenschutzaufsichten Muster und entsprechende Erläuterungen entwickelt, die zur Verwendung bereitgestellt worden sind. (Homepages der Diözesandatenschutzaufsichten – Muster/Formulare)

Die Bezugnahme im Text auf die KDO ist auf das Gesetz über den Kirchlichen Datenschutz (KDG) umzustellen.

Arbeitshilfe

KDO-DVO	Anmerkung zur Weitergeltung
III abzugeben. Die Urschrift der Verpflichtungserklärung wird zu den Personalakten der bei der Datenverarbeitung tätigen Personen genommen, welche eine Ausfertigung der Erklärung erhalten.	
(3) Die Verpflichtung auf das Datengeheimnis erfolgt durch den Dienstvorgesetzten der in der Datenverarbeitung tätigen Personen oder einen von ihm Beauftragten.	
III. Zu § 4 KDO:	***Neu: § 5 KDG***
(1) Die schriftliche Verpflichtungserklärung der bei der Datenverarbeitung tätigen Personen gemäß § 4 Satz 2 KDO hat zum Inhalt, 1. Angaben zur Identifizierung (Vor- und Zuname, Geburtsdatum und Anschrift sowie Beschäftigungsdienststelle), 2. die Bestätigung, 1.1 dass auf die für den Aufgabenbereich des Mitarbeiters wesentlichen Grundsätze und im Übrigen auf die Texte in der jeweils gültigen Fassung sowie 1.2 auf die Möglichkeit der Einsichtnahme und etwaigen kurzfristigen Ausleihe dieser Texte hingewiesen wurde, 3. die Verpflichtung, die KDO und andere für ihre Tätigkeit geltende Datenschutzvorschriften in der jeweils gültigen Fassung sorgfältig einzuhalten, 4. die Bestätigung, dass sie über disziplinarrechtliche bzw. arbeitsrechtliche/rechtliche Folgen eines Verstoßes gegen die KDO belehrt wurden.	*„Verpflichtungserklärung“*
(2) Die schriftliche Verpflichtungserklärung ist von der bei der Datenverarbeitung tätigen Person unter Angabe des Ortes und des Datums der Unterschriftsleistung zu unterzeichnen.	*Die bisher abgegebenen Verpflichtungserklärungen nach dem alten Recht (KDO) bleiben uneingeschränkt gültig. Erforderlich ist allerdings eine Information durch den Verantwortlichen für die Mitarbeiterinnen und Mitarbeiter über die Veränderungen der Rechtsgrundlagen im kirchlichen Datenschutz.*
(3) Für die schriftliche Verpflichtungserklärung ist das Muster gemäß der Anlage zu verwenden.	
IV. Zu § 6 KDO:	
Anlage 1:	***Neu: § 26 ff. KDG***
Werden personenbezogene Daten automatisiert, verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden perso-	*Die Anlage 1 ist in der bisherigen Form nicht mehr anwendbar, weil §§ 26 ff. KDG andere Begriffe für die Beurteilung der technischen und organisatorischen Maßnahmen (TOM`s) gebrauchen. Insoweit ist es erforderlich, eine Ausrichtung*

KDO-DVO

nenbezogenen Daten oder Datenkategorien geeignet sind,

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

Anlage 2:

1.0 Aufgaben und Ziele dieser Anlage
Diese Anlage regelt den Einsatz von Arbeitsplatzcomputern in kirchlichen Stellen. Sie ist als Ergänzung zu § 6 der Anordnung über den Kirchlichen Datenschutz (KDO) und den zu ihr ergangenen bereichsspezifischen Datenschutzregelungen in ihren jeweils gelten-den Fassungen anzusehen. Die nachstehende Anlage 2 zu § 6 KDO und die IT-Richtlinien zur Umsetzung der

Anmerkung zur Weitergeltung

der Schutzmaßnahmen unter Berücksichtigung der neuen Ziele und Begriffe vorzunehmen. Als „Leitlinien“ können die bisherigen Kategorien allerdings noch Verwendung finden.

Die Bezugnahme im Text auf die KDO ist auf das Gesetz über den Kirchlichen Datenschutz (KDG) umzustellen.

Arbeitshilfe

KDO-DVO	Anmerkung zur Weitergeltung
Anlage 2 gelten nur insoweit, als keine weitergehenden Regelungen zu Datenschutz und Datensicherheit erlassen sind.	
2.0 Arbeitsplatzcomputer/Datenverarbeitungsanlage • Arbeitsplatzcomputer (APC) im Sinne dieser DVO sind alle selbständigen Systeme der Datenverarbeitung, die von einer kirchlichen Stelle im Sinne des § 1 Abs. 2 KDO zur Erfüllung ihrer Aufgaben genutzt werden. • Sie können als Einzelgerät (Stand-Alone-PC) oder in Verbindung mit anderen APC (Netzwerken) bzw. anderen Systemen als Datenverarbeitungsanlage installiert sein. • Als APC sind z.B. auch tragbare Geräte (Laptops bzw. Notebooks oder Net-books), Tabletcomputer und Mobiltelefone sowie Drucker bzw. Kopierer mit eigener Speichereinheit zu behandeln.	
3.0 Allgemeine Grundsätze 3.1 Verantwortlichkeit der Mitarbeiter • Mitarbeiter im Sinne dieser Anlage sind über die in § 2 Abs. 12 KDO genannten Beschäftigten hinaus auch ehrenamtlich für kirchliche Stellen tätige Personen, die APC verwenden. • Jeder Mitarbeiter trägt die datenschutzrechtliche Verantwortung für eine vorschriftsmäßige Ausübung seiner Tätigkeit. Es ist ihm untersagt, personenbezogene Daten zu einem anderen als dem in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck zu verarbeiten oder zu übermitteln.	*Zu beachten ist bei den allgemeinen Grundsätzen auch die „Nachweispflicht“ der Verantwortlichen und Auftragsverarbeiter im Hinblick auf die eingesetzten technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten.*
3.2 Verantwortlichkeit der Dienststellenleiter • Die jeweils als Dienststellenleiter verantwortliche Person ist durch den Generalvikar oder durch die sonst vorgesetzte Dienststelle zu bestimmen. • Der Dienststellenleiter legt fest, welche im Sinne der KDO schutzwürdigen Daten auf Datenverarbeitungsanlagen gespeichert und verarbeitet werden. • Ihm obliegt die zutreffende Einordnung der jeweiligen Daten in die Datenschutzklassen nach diesen Richtlinien. • Der Dienststellenleiter klärt die Mitarbeiter über die Gefahren, die aus der Nutzung einer Datenverarbeitungsanlage erwachsen, sowie über den möglichen Schaden, der kirchlichen Einrichtungen aus einer Datenschutzverletzung erwachsen kann, auf. • Der Dienststellenleiter stellt sicher, dass ein Konzept zur datenschutzrechtlichen Ausgestaltung der Datenverarbeitungsanlagen erstellt wird.	*Anpassung an die neuen Begrifflichkeiten: „Verantwortlicher“ statt „Dienststellenleiter“*

KDO-DVO

- Der Dienststellenleiter kann seine Aufgaben und Befugnisse nach dieser Durchführungsverordnung durch schriftliche Anordnung auf geeignete Mitarbeiter übertragen.

3.3 Technische und organisatorische Maßnahmen
Mit der Eingabe, Speicherung, Verarbeitung und Nutzung personenbezogener Daten auf Anlagen der elektronischen Datenverarbeitung darf erst begonnen werden, wenn die Daten verarbeitende Stelle die nach der Anlage zu § 6 KDO und die nach dieser Richtlinie erforderlichen technischen und organisatorischen Maßnahmen zum Schutz dieser Daten getroffen hat.

3.4 Mindestanforderungen
Unabhängig vom Grad der Schutzbedürftigkeit der Daten sind dabei zumindest folgende Maßnahmen zu treffen:

- Das nach § 3 a Abs. 4 KDO zu führende Verzeichnis hat darüber hinaus den regelmäßigen Nutzer, den Standort und die interne Kennzeichnungs-Nummer zu enthalten.
- Alle bei der Verarbeitung personenbezogener Daten beteiligten Personen haben die Verpflichtungserklärung gemäß § 4 Abs. 2 Satz l KDO abzu-geben. Den Mitarbeitern, die die Verpflichtungserklärung unterschrieben haben, sind die jeweils gültige Anordnung über den kirchlichen Datenschutz, etwaige Verordnungen, Dienstanordnungen oder Dienstvereinbarungen und die in ihrem Arbeitsbereich zu beachtenden bereichsspezifischen Datenschutzregelungen (Schulen, Krankenhäuser, Friedhöfe etc.) in geschäftsüblicher Weise zugänglich zu machen.
- Es ist sicherzustellen, dass auf dienstlich genutzten Anlagen der elektronischen Datenverarbeitung ausschließlich autorisierte Programme zu dienstlichen Zwecken verwendet werden. Die Benutzung privater Programme ist unzulässig.
- Werden Daten aus den Melderegistern der kommunalen Meldebehörden in kirchlichen Rechenzentren verarbeitet, so orientieren sich die Schutz-maßnahmen an den BSI-IT-Grundschutzkatalogen. Rechenzentren im Sinne dieser Vorschrift sind die

Anmerkung zur Weitergeltung

Diese Regelung ist u.E. dann nicht mehr frei von erheblichen rechtlichen Bedenken, wenn der Verantwortliche seine Aufgaben und Befugnisse auf den betrieblichen Datenschutzbeauftragten im Rahmen seiner sonstigen Tätigkeiten überträgt. Eine Kollision mit den Aufgaben des bDSB nach den Bestimmungen des § 38 KDG ist nicht unwahrscheinlich. Es ist jedenfalls im Einzelfall sehr genau zu prüfen, ob Interessenskollisionen gegeben sein könnten.

Zu beachten ist auch hier die „Nachweispflicht“ der Verantwortlichen und Auftragsverarbeiter im Hinblick auf die eingesetzten technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten.

KDO-DVO	Anmerkung zur Weitergeltung
für den Betrieb von größeren, zentral in mehreren Dienststellen eingesetzten Informations- und Kommunikationssystemen erforderlichen Einrichtungen.	
4.0 Datenschutzklassen • Das Ausmaß der möglichen Gefährdung personenbezogener Daten bestimmt Art und Umfang der Sicherungsmaßnahmen. Zur Erleichterung der Einordnung bedient sich diese Anlage der Definition dreier Datenschutzklassen, die sich aus der Art der zu verarbeitenden Daten ergeben. Dem Dienststellenleiter, der die Einordnung vornimmt, steht es frei, aus Gründen des Einzelfalles die zu verarbeitenden Daten anders einzuordnen als hier vorgesehen. Diese Gründe sollen kurz dokumentiert werden. • Bei der Einordnung in die einzelnen Datenschutzklassen ist auf die Daten abzustellen, die vom Benutzer bewusst bearbeitet und gespeichert werden.	*Die Einteilung in verschiedene Datenschutzklassen beruht u.E. auf der Notwendigkeit der Risikobewertung bei der Verarbeitung personenbezogener Daten nach dem KDG.* *Anpassung an die neuen Begrifflichkeiten: „Verantwortlicher“ statt „Dienststellenleiter“*
4.1 Datenschutzklasse I Zur Datenschutzklasse I gehören personenbezogene Daten, deren Missbrauch keine besonders schwer wiegende Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören insbesondere Adressangaben ohne Sperrvermerke, z. B. Berufs-, Branchen- oder Geschäftsbezeichnungen.	
4.2 Datenschutzklasse II Zur Datenschutzklasse II gehören personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten, usw.	
4.3 Datenschutzklasse III Zur Datenschutzklasse III gehören personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören z.B. Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen, usw. sowie Adressangaben mit Sperrvermerken.	
4.4 Nicht elektronisch zu verarbeitende Daten Daten, deren Kenntnis dem Beicht- oder Seelsorgegeheimnis unterliegen sowie Daten über die Annahme	

KDO-DVO	Anmerkung zur Weitergeltung
einer Person an Kindes Statt (Adoptionsgeheimnis) sind in besonders hohem Maße schutzbedürftig. Ihre Ausspähung oder Verlautbarung würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen. Daher dürfen diese Daten nicht auf APC verarbeitet werden, es sei denn, es handelte sich um aus dem staatlichen Bereich übernommene Daten.	
4.5 Einordnung in die Datenschutzklassen • Bei der Einordnung der zu speichernden personenbezogenen Daten in die vorgenannten Schutzklassen ist auch deren Zusammenhang mit anderen gespeicherten Daten, der Zweck ihrer Verarbeitung und das anzunehmende Missbrauchsinteresse zu berücksichtigen.	
• Die Einordnung spricht der Dienststellenleiter aus; er soll einen etwa bestellten betrieblichen Datenschutzbeauftragten und kann den Diözesandatenschutzbeauftragten dazu anhören.	*Anpassung an die neuen Begrifflichkeiten: „Verantwortlicher“ statt „Dienststellenleiter“*
• Wenn keine Einordnung festgelegt ist, gilt automatisch die Datenschutzklasse III, sofern nicht die Voraussetzungen der Ziffer 4.4 vorliegen.	
5.0 Besondere Gefahrenlagen 5.1 Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken Die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungssystemen zu dienstlichen Zwecken ist grundsätzlich unzulässig. Unter bestimmten Voraussetzungen kann sie als Ausnahme vom Dienststellenleiter genehmigt werden. Die Genehmigung erfolgt schriftlich unter Nennung der Gründe.	*Anpassung an die neuen Begrifflichkeiten: „Verantwortlicher“ statt „Dienststellenleiter“*
5.2 Fremdzugriffe Der Zugriff aus und von anderen Datenverarbeitungsanlagen durch Externe (z.B. Fremdfirmen, fremde Dienststellen) schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. Minimalanforderung ist eine Verpflichtung des Externen auf die KDO. Art und Umfang der Zugriffe sind auf ein Mindestmaß zu reduzieren und gesondert zu regeln.	
Für die Fernwartung gilt § 8 KDO entsprechend.	***Neu: § 29 Abs. 12 KDG*** *Bei der Prüfung oder Wartung automatischer Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag gilt § 29 KDG entsprechend.*

KDO-DVO	Anmerkung zur Weitergeltung
Anlage 3: **IT-Richtlinien zur Umsetzung von IV. Anlage 2 zu § 6 KDO der Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO):** Präambel Die IT-Richtlinien definieren einen Mindeststandard für den kirchlichen Datenschutz. Dieser dient auch dazu, die überdiözesane Zusammenarbeit zu erleichtern (Datenschutzkonformität). Die zu etablierenden Datenschutzklassen (DSK) sind sowohl auf personenbezogene als auch auf schützenswerte nicht personenbezogene Daten anzuwenden (z.B. auf Buchhaltungsdaten (= DSK II) und Kirchensteuerdaten (= DSK III)). 1. Nach den jeweiligen Datenschutzklassen erforderliche Maßnahmen Die zum Schutz der Daten erforderlichen Maßnahmen richten sich nach der Einordnung in eine von drei Datenschutzklassen (vgl. KDO-DVO IV. Anlage 2 zu § 6 KDO Pkt. 4.1 - 4.3). Die jeweils erforderlichen Maßnahmen sind auch bei Auftragsdatenverarbeitung einzuhalten; die Kontrollierbarkeit der Durchführung der Maßnahmen durch den Auftraggeber ist sicher zu stellen.	*Auch hier ist auf die Nachweispflicht aus § 26 Abs. 1 a. E. KDG zu achten.*
2. Maßnahmen in den Datenschutzklassen 2.1 Maßnahmen in Datenschutzklasse I Zum Schutz der in die Datenschutzklasse I einzuordnenden Daten ist ein Schutzniveau I zu definieren. Dieses setzt mindestens voraus: • Der Arbeitsplatzcomputer (APC) ist nicht frei zugänglich, z.B.: in einem abschließbaren Gebäude oder unter ständiger Aufsicht. • Die Anmeldung am APC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich. • Sicherungskopien der Datenbestände sind verschlossen aufzubewahren. • Vor der Weitergabe eines Datenträgers für einen anderen Einsatzzweck sind die auf ihm befindlichen Daten so zu löschen, dass ihre Wiederherstellung ausgeschlossen ist. • Nicht öffentlich verfügbare Daten sind nur dann weiter zu geben, wenn sie durch geeignete Schutzmaßnahmen geschützt sind. Die Art und Weise des Schutzes ist vor Ort zu definieren. 2.2 Maßnahmen in Datenschutzklasse II Zum Schutz der in die Datenschutzklasse II einzuordnenden Daten ist ein Schutzniveau II zu definieren. Dieses setzt mindestens voraus, dass neben dem	

KDO-DVO

Anmerkung zur Weitergeltung

Schutzniveau I mindestens folgende Voraussetzungen gegeben sind:

- Die Anmeldung am APC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich, dessen Erneuerung in regelmäßigen Abständen systemseitig vorgesehen werden muss.
- Das Laden des Betriebssystems der Datenverarbeitungsanlage darf nur mit dem dafür bereit gestellten Betriebssystem erfolgen (Boot-Schutz). Diese BIOS-Einstellung ist durch ein besonderes Passwort zu sichern, das nur dem Systemverwalter bekannt ist.
- Im Mehrbenutzer- oder Netzwerkbetrieb und bei einer PC/Host-Koppelung ist eine abgestufte Rechteverwaltung erforderlich. Der Anwender sollte keine Administrationsrechte erhalten.
- Sicherungskopien und Ausdrucke der Datenbestände sind vor Fremdzugriff und vor der gleichzeitigen Vernichtung mit den Originaldaten zu schützen.
- Die Daten der Schutzklasse II sind auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu speichern, sofern keine begründeten Ausnahmefälle gegeben sind. Die jeweils beteiligten Systeme und Transportwege sind nach dem aktuellen Stand der Technik angemessen zu schützen.
- Eine Speicherung auf mobilen Datenträgern darf nur erfolgen, wenn diese mit einem geeigneten Zugriffsschutz ausgestattet sind.

2.3 Maßnahmen in Datenschutzklasse III
Zum Schutz der in die Datenschutzklasse III einzuordnenden Daten ist ein Schutzniveau III zu definieren. Dieses setzt voraus, dass neben dem Schutzniveau II mindestens folgende Voraussetzungen gegeben sind:

Soweit es unvermeidlich ist, dass Daten der Datenschutzklasse III auf mobilen Geräten und Datenträgern gespeichert werden müssen, sind diese Daten verschlüsselt abzuspeichern. Das Verschlüsselungsverfahren ist nach dem aktuellen Stand der Technik angemessen auszuwählen.

Besonderes Augenmerk muss dabei auf langfristige und nutzerunabhängige Lesbarkeit der zu speichernden Daten gelegt werden. So müssen z.B. bei verschlüsselten Daten die Sicherheit des Schlüssels und die erforderliche Entschlüsselung auch im Datensicherungskonzept berücksichtigt werden.

Anm.: Dies gilt nicht für die Festplatten von Druckern,

KDO-DVO	Anmerkung zur Weitergeltung
sofern sichergestellt ist, dass diese nicht von einem Benutzerarbeitsplatz ausgelesen werden können.	
3. Maßnahmen zur Datensicherung Der Dienststellenleiter ist für die Erstellung und Umsetzung eines Datensicherungskonzeptes verantwortlich. Besonderes Augenmerk muss dabei auf die langfristige und nutzerunabhängige Lesbarkeit der zu speichernden Daten in der Datensicherung gelegt werden. Zum Schutz des personenbezogenen Datenbestandes vor dessen Verlust sind regelmäßige Datensicherungen erforderlich. Dabei sind u.a. folgende Aspekte mit zu berücksichtigen:	*Anpassung an die neuen Begrifflichkeiten: „Verantwortlicher“ statt „Dienststellenleiter“*
3.1 Sicherungskopien der verwendeten Programme Es sind Sicherungskopien der verwendeten Programme in allen verwendeten Versionen anzulegen und möglichst von den Originaldatenträgern der Programme und den übrigen Datenträgern getrennt aufzubewahren.	
3.2 Zeitabstände bei der Datensicherung Die Datensicherung soll in Umfang und Zeitabstand anhand der entstehenden Auswirkungen eines Verlustes der Daten festgelegt werden.	
4. Besondere Gefahrenlagen 4.1 Fernwartung Eine Fernwartung von APC durch externe Unternehmer schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. Sie darf daher nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde und der Verlauf sowie das Ende mindestens überprüfbar sind.	
4.2 Auftragsdatenverarbeitung Werden personenbezogene Daten auf zentralen Systemen außerhalb des Geltungsbereiches der Anordnung über den kirchlichen Datenschutz (KDO) gespeichert (z.B. Public Cloud), sind die Auftragnehmer auf die KDO zu verpflichten. Ergänzend ist sicher zu stellen, dass der physikalische Speicherort der Daten ausschließlich im Geltungsbereich des BDSG liegt. Sobald eine einheitliche europäische Datenschutzverordnung in Kraft ist, wird auf deren Geltungsbereich abgestellt.	
4.3 Nutzung privater Datenverarbeitungssysteme Werden im zu genehmigenden Einzelfall personenbezogene Daten auf privaten Datenverarbeitungsanlagen verarbeitet oder werden personenbezogene Daten auf private E-Mail-Konten geleitet, sind die Nutzer schriftlich auf die Einhaltung dieser IT-Richtlinie zu	*Die Regelung in Zf. 4.3 ist u.E. insgesamt kritisch zu sehen, da der Verantwortliche auch bei Speicherung der Daten auf den privaten Systemen oder in privaten E-Mail-Konten für die technisch-organisatorischen Maßnahmen zum Schutz*

KDO-DVO	Anmerkung zur Weitergeltung
verpflichten. In dieser Erklärung verpflichten sich die Nutzer, betreffende personenbezogene Daten durch die Dienststelle und auf deren Anforderung löschen zu lassen. Ergänzend soll dem Nutzer eine spezifische Handlungsanleitung ausgehändigt werden, um den Schutz dieser Daten zu gewährleisten. Der Dienststelle wird das Recht eingeräumt, die gespeicherten dienstlichen Daten aus wichtigem Grund auch ohne Einwilligung des Nutzers zu löschen und, falls dies unumgänglich ist, die auf dem APC gespeicherten privaten Daten zu löschen.	*der Daten nach § 26 KDG verantwortlich bleibt. Dies dürfte im Regelfall nicht oder nur schwer umzusetzen sein.*
4.4 Wartungsarbeiten in der Dienststelle durch externe Auftragnehmer Bei der Durchführung von Wartungsarbeiten innerhalb der Dienststelle ist mit besonderer Sorgfalt darauf zu achten und nach Möglichkeit auch technisch sicherzustellen, dass keine Kopien der personenbezogenen Datenbestände gefertigt werden können. Muss dem Wartungsdienst bei Vornahme der Arbeiten ein Passwort mitgeteilt werden, ist dieses sofort nach deren Beendigung zu ändern.	
4.5 Wartungsarbeiten außerhalb der Dienststelle Die Durchführung von Wartungsarbeiten in den Räumen eines Fremdunter-nehmens auf Datenträgern mit Daten der DSK III sollte nur in besonderen Ausnahmefällen erfolgen. Das Fremdunternehmen ist vor Beginn der Wartungsarbeiten auf die Einhaltung der KDO zu verpflichten.	*Es ist auf die Einhaltung des KDG zu verpflichten.*
4.6 Verschrottung und Vernichtung von Datenträgern Es sind Maßnahmen bei der Verschrottung bzw. Vernichtung von Datenträgern zu ergreifen, die die Lesbarkeit oder Wiederherstellbarkeit der Datenträger zuverlässig ausschließen.	
4.7 Passwortlisten der Systemverwaltung Der Systemverwalter muss alle nicht zurücksetzbaren Passwörter (z.B. BIOS- und Administrationspasswörter) besonders gesichert aufbewahren.	
V. Zu § 12 Abs. 3 KDO:	***Neu: 10 Abs. 3 KDG.***
(1) Die Unterrichtung des Betroffenen (§ 2 Abs. 1 KDO) über eine Übermittlung gemäß § 12 Abs. 3 Satz 1 KDO erfolgt schriftlich.	*Die Vorschrift ist im Vergleich zu § 12 Abs. 3 KDO inhaltlich unverändert. Es sind aber ggf. die Informationspflichten aus den §§ 15, 16 KDG zu beachten.*
(2) Sie enthält 1. die Bezeichnung der übermittelnden Stelle einschließlich der Anschrift,	

KDO-DVO	Anmerkung zur Weitergeltung
2. die Bezeichnung des Dritten, an den die Daten übermittelt werden, einschließlich der Anschrift, 3. die Bezeichnung der übermittelten Daten.	
VI. Zu § 13 Abs. 1 KDO:	***NEU: § 17 KDG:***
(1) Der Antrag des Betroffenen (§ 2 Abs. 1 KDO) auf Auskunft ist schriftlich an die verantwortliche Stelle (§ 2 Abs. 8 KDO) zu richten oder dort zu Protokoll zu erklären.	*Das Auskunftsrecht der betroffenen Person ist jetzt in § 17 KDG geregelt.* *Ein Antrag in schriftlicher Form wird vom KDG nicht vorausgesetzt, sollte aus Nachweisgründen bei der betroffenen Person aber angeregt werden.*
(2) Der Antrag soll die Art der personenbezogenen Daten, über die Auskunft begehrt wird, näher bezeichnen.	*§ 17 KDG sieht keine zwingende Angabe der Daten der betroffenen Person vor, für die Auskunft begehrt wird. Der Verantwortliche wird aber zumindest die Daten erfragen müssen, die ihm im konkreten Fall eine Identifizierung der Person ermöglichen, da auch eine Auskunftserteilung an eine falsche Person bzw. eine Auskunft über Daten einer anderen Person eine Datenschutzverletzung darstellt.*
Der Antrag auf Auskunft über personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, muss Angaben enthalten, die das Auffinden der Daten ermöglichen.	*Diese Regelung ist so u.E. nicht mehr anwendbar. § 17 Abs. 9 KDG regelt für die dort genannten Fälle die Pflicht zur Angabe weiterer Daten durch die anfragende Person. Andere Fälle hat der Gesetzgeber nicht geregelt, so dass diese Vorschrift für Einrichtungen im Sinne des § 3 Abs. 1 lit. b) oder c) KDG nicht greift.*
(3) Der Antrag kann beschränkt werden auf Auskunft über 1. die zur Person des Betroffenen gespeicherten Daten oder 2. die Herkunft dieser Daten oder 3. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben worden sind oder 4. den Zweck, zu dem diese Daten gespeichert sind.	*Der Antrag auf Auskunft kann sich auf eine Teilmenge der in den lit. a) bis h) des § 17 KDG genannten Informationen beschränken.*
(4) Vorbehaltlich der Regelung in § 13 Abs. 3 KDO wird die Auskunft in dem beantragten Umfang von der verantwortlichen Stelle (§ 2 Abs. 8 KDO) schriftlich erteilt.	*Die Fälle, in denen eine Auskunft unterbleiben kann, sind jetzt in § 17 Abs. 5 bis 8 KDG aufgezählt. Im Fall des § 17 Abs. 3 Satz 3 KDG kann die Antwort auch auf elektronischem Weg erfolgen.*

KDO-DVO	Anmerkung zur Weitergeltung
(5) Wenn die Erteilung der beantragten Auskunft gemäß § 13 Abs. 2 oder 3 KDO zu unterbleiben hat, so ist dies dem Antragsteller schriftlich mitzuteilen. Die Versagung der beantragten Auskunft soll begründet werden. Für den Fall, dass eine Begründung gemäß § 13 Abs. 4 KDO nicht erforderlich ist, ist der Antragsteller darauf hinzuweisen, dass er sich an den Diözesandatenschutzbeauftragten wenden kann; die Anschrift des Diözesandatenschutzbeauftragten ist ihm mitzuteilen.	*Diese Regelung ist so u.E. nicht mehr anwendbar. Die entsprechenden Vorgaben sind jetzt in § 17 Abs. 7 und 8 KDG aufgezählt. Diese Vorgaben sind zu beachten.*
VII. Zu § 13 a KDO:	
(1) Die Benachrichtigung des Betroffenen (§ 2 Abs. 1 KDO) gemäß § 13 a Abs. 1 KDO erfolgt, soweit die Pflicht zur Benachrichtigung nicht nach § 13 a Abs. 2 und 3 entfällt, schriftlich durch die verantwortliche Stelle.	*Diese Regelung ist u.E. nicht mehr anwendbar. Die Vorgaben für eine Benachrichtigung der betroffenen Person bei mittelbarer Datenerhebung sind jetzt ausführlich in § 16 KDG geregelt.*
(2) Sie enthält 1. die zur Person des Betroffenen gespeicherten Daten, 2. die Bezeichnung der verantwortlichen Stelle, 3. den Zweck, zu dem die Daten erhoben, verarbeitet oder genutzt werden. 4. die Empfänger oder Kategorien von Empfängern, soweit der Betroffene nicht mit der Übermittlung an diese rechnen muss.	
VIII. Zu § 14 KDO:	
(1) Der Betroffene (§ 2 Abs. 1 KDO) kann schriftlich beantragen, ihn betreffende personenbezogene Daten zu berichtigen oder zu löschen. Der Antrag ist schriftlich an die Stellen gemäß § 1 Abs. 2 Nr. 2 und 3, im Falle des § 1 Abs. 2 Nr. 1 an das Bistum zu richten.	*Diese Regelung ist u.E. nicht mehr anwendbar. Das Recht auf Berichtigung ist nun in § 18 KDG und das Recht auf Löschung in § 19 KDG geregelt. In beiden Fällen ist der Anspruch beim Verantwortlichen im Sinne von § 4 Zf. 9 KDG geltend zu machen. Ein Antrag in schriftlicher Form wird vom KDG nicht vorausgesetzt, sollte aus Nachweisgründen bei der betroffenen Person aber angeregt werden.*
(2) In dem Antrag auf Berichtigung sind die Daten zu bezeichnen, deren Unrichtigkeit behauptet wird. Der Antrag muss Angaben über die Umstände enthalten, aus denen sich die Unrichtigkeit der Daten ergibt.	*Diese Regelung ist u.E. nicht mehr anwendbar. § 18 KDG sieht dies nicht als Voraussetzung für den Antrag auf Berichtigung vor. Gleichwohl wird in der Praxis die Bezeichnung der zu berichtigenden Daten durch die betroffene Person überwiegend notwendig sein, da die Berichtigung für den Verantwortlichen nicht immer offensichtlich sein wird.*

KDO-DVO	Anmerkung zur Weitergeltung
(3) In dem Antrag auf Löschung sind die personenbezogenen Daten zu bezeichnen, deren Speicherung für unzulässig gehalten wird. Der Antrag muss Angaben über die Umstände enthalten, aus denen sich die Unzulässigkeit der Speicherung ergibt.	*Diese Regelung ist u.E. nicht mehr anwendbar. § 19 KDG sieht dies nicht als Voraussetzung für den Antrag auf Löschung vor. Gleichwohl wird in der Praxis die Bezeichnung der zu löschenden Daten durch die betroffene Person – abhängig vom Grund der Löschung im Sinne von § 19 Abs. 1 KDG – notwendig sein, da der Grund für das Löschungsbegehren und die zu löschenden Daten für den Verantwortlichen nicht immer offensichtlich sein werden.*
(4) Die zuständige Stelle entscheidet schriftlich über Anträge gemäß Abs. 1. Die Entscheidung ist dem Antragsteller bekannt zu geben. Im Falle des § 14 Abs. 8 KDO sind ihm die Stellen anzugeben, die von der Berichtigung, Löschung oder Sperrung verständigt worden sind. Ist eine Verständigung aufgrund des § 14 Abs. 8 KDO unterblieben, sind dem Antragsteller die Gründe dafür mitzuteilen.	*Der Regelungsinhalt des § 14 Abs. 8 KDO ist jetzt in § 21 KDG und in § 19 Abs. 2 KDG enthalten. Soweit auf die Vorschrift des § 14 Abs. 8 KDO Bezug genommen wird, sind diese beiden Regelungen heranzuziehen.*
(5) Der Widerspruch gemäß § 14 Abs. 5 KDO ist schriftlich oder zur Niederschrift bei der verantwortlichen Stelle (§ 2 Abs. 8 KDO) einzulegen. Die Umstände, aus de-nen sich das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation ergibt, sind von dem Betroffenen darzulegen. Die verantwortliche Stelle entscheidet über den Widerspruch in geeigneter Form. Die Entscheidung ist dem Betroffenen bekannt zu geben.	*Diese Regelung ist so u.E. nicht mehr anwendbar. § 23 KDG enthält für die dort geregelten Fälle entsprechende Vorgaben, wie mit den Ersuchen umzugehen ist.*
II. Inkrafttreten Die vorstehende Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz für das Erzbistum Paderborn (KDO-Durchführungsverordnung – KDO-DVO) tritt zum 1. November 2015 in Kraft. Gleichzeitig tritt die KDO-DVO vom 8. September 2003 (KA 2003, Nr. 195) außer Kraft.	
Anlagen zur KDO-DVO 1. Zu Abschnitt I. KDO-DVO (§ 3 a KDO Meldung von Verfahren automatisierter Verarbeitung) Die Notwendigkeit für die in den nachfolgenden Formularen (Muster 1 und Muster 2) geforderten Angaben ergibt sich aus § 3 a KDO. Für jedes automatisierte Verfahren einer verantwortlichen Stelle füllt der	*Zur weiteren Anwendbarkeit siehe oben die Erläuterungen zu § 3a KDO.*

KDO-DVO

Rechtsträger (§ 1 Abs. 2 KDO) ein Formular nach Muster 1 und Muster 2 aus.

Muster 1

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

1. Name und Anschrift
1.1 des Rechtsträgers (§ 1 Abs. 2 KDO) (z.B. Kirchengemeinde)
1.2 der verantwortlichen Stelle (Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt [§ 2 Abs. 8 KDO]) (z.B. Kindergarten der Kirchengemeinde)

2. Vertretung der verantwortlichen Stelle
2.1 der nach der Verfassung (Statut, Geschäftsordnung, Satzung) berufene Lei-ter der verantwortlichen Stelle (z.B. Leiterin des Kindergartens der Kirchengemeinde)
2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen (z.B. beauftragte Gruppenleiterin im Kindergarten der Kirchengemeinde)

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

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

4. Betroffene Personengruppen und Daten oder Datenkategorien
4.1 Beschreibung der betroffenen Personengruppen (z. B. Arbeitnehmer, Gemeindemitglieder, Patienten usw.)
4.2 Beschreibung der diesbezüglichen Daten oder Datenkategorien (Mit „Daten“ sind „personenbezogene Daten“ i. S. d. § 2 Abs. 1 KDO gemeint, wie z.B. Name, Anschrift, Geburtsdatum, Religionszugehörigkeit. Grundsätzlich reicht jedoch die Angabe von Datenkategorien, z.B. Personaldaten, aus. Sogenannte „besondere Arten personenbezogener Daten“ (vgl. § 2 Abs. 10 KDO) sind entsprechend anzugeben.)

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

Anmerkung zur Weitergeltung

KDO-DVO	Anmerkung zur Weitergeltung

6. Regelfristen für die Löschung der Daten

7. Geplante Datenübermittlung ins Ausland

Ort, Datum, Unterschrift

Muster 2

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

1. Name und Anschrift
1.1 des Rechtsträgers (§ 1 Abs. 2 KDO) (z.B. Kirchengemeinde)
1.2 der verantwortlichen Stelle (Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt [§ 2 Abs. 8 KDO]) (z.B. Kindergarten der Kirchengemeinde)

2. Vertretung der verantwortlichen Stelle
2.1 der nach der Verfassung (Statut, Geschäftsordnung, Satzung) berufene Lei-ter der verantwortlichen Stelle (z.B. Leiterin des Kindergartens der Kirchengemeinde)
2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen (z.B. beauftragte Gruppenleiterin im Kindergarten der Kirchengemeinde)

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

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

4. Zugriffsberechtigte Personen

Ort, Datum, Unterschrift

KDO-DVO

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

Verpflichtungserklärung

Ich verpflichte mich,

1. die Anordnung über den kirchlichen Datenschutz für das Erzbistums Paderborn (KDO) sowie die anderen für meine Tätigkeit geltenden Datenschutzregelungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen in ihren jeweils geltenden Fassungen sorgfältig einzuhalten und bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen hingewiesen wurde. Ich wurde ferner darauf hingewiesen, dass die KDO und die Texte der übrigen für meine Tätigkeit geltenden Datenschutzvorschriften bei ..... eingesehen und auch für kurze Zeit ausgeliehen werden können.

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

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

Diese Erklärung wird zu den Akten genommen.

Vor- und Zuname, Anschrift:

Ort, Datum Unterschrift

Anmerkung zur Weitergeltung

Sofern im Text die Hinweise auf die KDO durch Hinweise auf das KDG ersetzt werden, kann das Formular weiter genutzt werden. Die Diözesandatenschutzbeauftragten halten aber auch ein neues, auf das KDG angepasstes Formular auf ihren Internetseiten zum Abruf bereit.

„Was bedeutet eigentlich ...“

Erläuterung zu Abkürzungen in den Anmerkungen

bDSB	betrieblicher Datenschutzbeauftragter
DDSB	Diözesandatenschutzbeauftragter
KDG	Gesetz über den Kirchlichen Datenschutz
KDO	Anordnung über den kirchlichen Datenschutz
KDO-DVO	Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz
TOM	technische und organisatorische Maßnahmen

Weitere Arbeitshilfen der Konferenz:

Formulierungshilfe zu den Informationspflichten

Leitfaden zur elektronischen Kommunikation

Formulierungshilfe zur Verpflilchtungserklärung nach § 5 KDG

Formulierungshilfe Vertrag über vertragsärztliche Leistungen

Formulierungshilfe Vertrag Fernwartung

Praxishilfen der Konferenz:

01 Wichtige Schritte zur Umsetzung eines gesetzeskonformen Datenschutzes

02 Der betriebliche Datenschutzbeauftragte nach dem KDG

03 Verantwortlichkeiten nach dem KDG

04 Auftragsverarbeitung nach dem KDG

05 Verzeichnis der Verarbeitungstätigkeiten nach dem KDG

06 Betroffenenrechte nach dem KDG

07 Transparenz- und Dokumentationspflichten nach dem KDG

08 Datenübermittlung in Drittländer

09 Befugnisse und Sanktionsmöglichkeiten der Aufsicht nach dem KDG

10 Umgang mit Datenpannen nach dem KDG

11 Datenschutzfolgeabschätzung nach dem KDG

12 Neue Anforderungen an die IT-Sicherheit nach dem KDG

13 Datenschutzorganisation und -managementsysteme nach dem KDG

14 Der Rechtsweg nach der KDSGO

15 Technischer Datenschutz nach dem KDG

16 Begriffe im neuen KDG

17 Rechtmäßigkeit der Verarbeitung/Einwilligung

18 Nutzung der Daten für Werbezwecke

Diese Arbeitshilfe wird gemeinsam herausgegeben von

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Diözesandatenschutz-
beauftragter für die nord-
deutschen (Erz-)Diözesen

Diözesandatenschutz-
beauftragter für die ost-
deutschen (Erz-)Diözesen

Katholisches
Datenschutzzentrum

Diözesandatenschutzbeauftragter für die
nordrhein-westfälischen (Erz-)Diözesen

Diözesandatenschutzbeauftragter
für die bayerischen (Erz-)Diözesen

Diözesandatenschutzbeauftragte der (Erz-)Diözesen Freiburg,
Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier