KDG-Praxishilfe 3

Verantwortlichkeiten

nach dem neuen Gesetz über den Kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 3

Verantwortlichkeiten nach dem Kirchlichen Datenschutzgesetz (KDG)

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: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Autor dieser Praxishilfe:
Der Diözesandatenschutzbeauftragte für die bayerischen (Erz-)Bistümer

Diese Praxishilfe der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands dient als erste Orientierung, wie nach Auffassung der Diözesandatenschutzbeauftragten das neue Gesetz über den kirchlichen Datenschutz (KDG) im praktischen Vollzug angewendet werden sollte. Sie kann noch keine verbindliche Auslegung bieten, sondern stellt die gegenwärtige Interpretation der neuen Vorschriften durch die Diözesandatenschutzbeauftragten dar.

Revision 2.0/ 22.12.2017

Verantwortlichkeiten nach dem Kirchlichen Datenschutzgesetz (KDG)

Begriffsbestimmung

Ausgangspunkt ist die Begriffsbestimmung in § 4 Abs. 1 Nr. 9 KDG:

> *„Verantwortlicher" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; […]*

Der Begriff ersetzt denjenigen der verantwortlichen Stelle im Sinne des § 2 Abs. 1 Nr. 8 Anordnung über den kirchlichen Datenschutz (KDO). Es hat sich jedoch im Prinzip an der Regelung nur wenig geändert, sieht man einmal davon ab, dass nunmehr im Gesetzestext ganz ausdrücklich auf diejenige natürliche Person Bezug genommen wird, die zur Entscheidung berufen ist. Sie ist auch diejenige, die letztlich für die Folgen der Datenschutzverletzungen haftet und der Androhung von Schadensersatzpflichten (§ 50 KDG) und Geldbußen (§ 51 KDG) ausgesetzt ist. Vom Betroffenen kann sie direkt im Verfahren vor dem Datenschutzgericht in Anspruch genommen werden (§ 49 KDG).

Der **Verantwortliche** in diesem Sinne ist zentrale Figur des Datenschutzmanagements. Ihm obliegen grundsätzlich alle Pflichten, die aus der Datenerfassung und -speicherung erwachsen, während der betriebliche Datenschutzbeauftragte ihm nur assistierend zur Seite steht und selber keine anderen Pflichten übernimmt als diejenige, den Datenschutz zu fördern. Die in § 31 – 35 KDG näher bezeichneten Pflichten wird der Verantwortliche regelmäßig zwar auch im Zusammenwirken mit dem betrieblichen Datenschutzbeauftragten erfüllen, doch trifft ihn die Verantwortung alleine.

Die EU-Datenschutz-Grundverordnung stellt an zahllosen Positionen den Verantwortlichen mit dem Auftragsverarbeiter gleich. Diese Gleichstellung hatte im KDG teilweise zu unterbleiben, weil externe Auftragsverarbeiter kirchlicher Dienststellen nicht ohne Weiteres selber dem KDG unterliegen. Es können zwar die Pflichten, die sich aus dem KDG für sie ergeben, Vertragsbestandteil werden, doch führt dies nur zu einer schuldrechtlichen Ausgestaltung des Vertrages dahingehend, dass die kirchliche Dienststelle vom

Auftragsverarbeiter die Erfüllung der Pflichten verlangen kann. Soweit kirchliche Dienststellen selbst Auftragsverarbeiter sind, greift aber wieder der Begriff des Verantwortlichen.

Wie sich schon aus der oben bezeichneten Definition ergibt, können bei der Verarbeitung personenbezogener Daten mehrere Verantwortliche mitwirken. Es sind auch kombinierte Mitwirkungsmöglichkeiten denkbar, zum Beispiel zwischen einer Behörde und einer natürlichen Person. Kommt es dann zu einer Datenschutzverletzung, greifen im Hinblick auf die zu verhängenden Geldbußen je nach Willensrichtung der Beteiligten die Grundsätze über die Mittäterschaft. Im Hinblick auf den Schadensersatz haften die mehreren Beteiligten als Gesamtschuldner.

Die in der Begriffsdefinition mit der Gleichstellung von natürlichen und juristischen Personen erreichten Rechtszustände werden durch § 51 Abs. 6 KDG doch wieder unterschiedlichen Ergebnissen zugeführt. Gegen kirchliche Dienststellen wird an sich keine Geldbuße verhängt, wohl aber gegen natürliche Personen, welche in ihnen die Entscheidungshoheit hatten. Das KDG folgt damit einer Öffnungsklausel der EU-Datenschutz-Grundverordnung, die auch die Bundesrepublik Deutschland übernommen hat.

Die Verantwortlichkeit des betrieblichen Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte ist natürlich nicht in demselben Umfang für Datenschutzverletzungen haftbar, wie es der Verantwortliche selbst ist. Nach dem Gesetz hat der betriebliche Datenschutzbeauftragte darauf hinzuwirken, dass die Dienststelle datenschutzkonform handelt. Aus diesem Text ergeben sich Zweifel, ob das Handeln des betrieblichen Datenschutzbeauftragten überhaupt kausal für einen eventuell eintretenden Schaden sein kann. Der Grund dafür ist, dass der betriebliche Datenschutzbeauftragte nicht einen Erfolg schuldet, sondern lediglich eine Handlung. Allerdings geht die herrschende Meinung davon aus, dass eine entsprechende Haftung des betrieblichen Datenschutzbeauftragten existiert.

Sie ist unterschiedlich, je nachdem, ob es sich um einen sogenannten internen oder externen betrieblichen Datenschutzbeauftragten handelt. Der interne betriebliche Datenschutzbeauftragte ist ein Mitarbeiter der Dienststelle, der ganz oder teilweise von anderen Tätigkeiten freigestellt ist. Der Externe hingegen wird von der Dienststelle beauftragt, entsprechende Leistungen zu erbringen. Er muss weder die Anforderungen des § 36 Abs. 5 Satz 2 KDG erfüllen, noch hat er die Privilegien des § 35 Abs. 4 KDG.

Der externe betriebliche Datenschutzbeauftragte haftet für jede Art von Verschulden, also auch für einfache Fahrlässigkeit. Demgegenüber genießt der interne betriebliche Datenschutzbeauftragte die Haftungsprivilegien der „gefahrgeneigten“ Arbeit, d. h., er haftet grundsätzlich nur für grobe Fahrlässigkeit und Vorsatz. Ist er der Dienststelle gegenüber zum Schadensersatz verpflichtet, so wird zwischen dieser und ihm grundsätzlich der Schaden aufgeteilt, wenn nicht die Dienststelle den gesamten Schaden zu tragen hat.

Um den Datenschutzbeauftragten vor solchen Zahlungspflichten bestmöglich zu schützen, sind Vereinbarungen möglich, wonach die Dienststellen die Schadenersatzforderungen in den bezeichneten Fällen selbst tragen und den Datenschutzbeauftragten von der Haftung freistellen. Eine ebenso gute Möglichkeit wäre es, eine Berufshaftpflichtversicherung für den Datenschutzbeauftragten abzuschließen. Dies beschränkt sich jedoch auf den Versicherungseintritt bei grober Fahrlässigkeit; eine Freistellung für Vorsatz scheidet rechtlich aus.

Wichtige Vorschriften des KDG zur Verantwortlichkeit

Der Begriff „Verantwortlicher“ ist nicht nur einer der wichtigsten im KDG, sondern auch ein Wort, das in nahezu jeder Vorschrift des KDG wieder auftaucht. Eigentlich müssten hier also fast alle Vorschriften des KDG erscheinen, doch sollen nur die wichtigsten hervorgehoben werden; auch sie werden überwiegend nur im Auszug wiedergegeben.

Gesetzestext § 14, § 26, § 28, § 31, § 38 und § 51 KDG (VDD Beschlussfassung, teilweise in Auszügen)

§ 14
Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person innerhalb einer angemessenen Frist alle Informationen gemäß den §§ 15 und 16 und alle Mitteilungen gemäß den §§ 17 bis 24 und 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache, ggf. auch mit standardisierten Bildsymbolen, zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Minderjährige richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

[...]

§ 26
Technische und organisatorische Maßnahmen

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung unter anderem des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. Diese Maßnahmen schließen unter anderem ein:

a) die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

[...]

§ 28
Gemeinsam Verantwortliche

(1) Legen mehrere Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtungen gemäß diesem Gesetz erfüllt, insbesondere wer den Informationspflichten gemäß den §§ 15 und 16 nachkommt.

(2) Die Vereinbarung gemäß Absatz 1 enthält die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber der betroffenen Person. Über den wesentlichen die Verarbeitung personenbezogener Daten betreffenden Inhalt der Vereinbarung wird die betroffene Person informiert.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieses Gesetzes bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

§ 31
Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie des betrieblichen Datenschutzbeauftragten, sofern ein solcher zu benennen ist;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) gegebenenfalls die Verwendung von Profiling;

e) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

f) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation und der dort getroffenen geeigneten Garantien;

g) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

h) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 26 dieses Gesetzes.

(2) Jeder Auftragsverarbeiter ist vertraglich zu verpflichten, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen, das folgende Angaben zu enthalten hat:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines betrieblichen Datenschutzbeauftragten, sofern ein solcher zu benennen ist;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation und der dort getroffenen geeigneten Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 26 dieses Gesetzes.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche und der Auftragsverarbeiter stellen dem betrieblichen Datenschutzbeauftragten und auf Anfrage der Datenschutzaufsicht das in den Absätzen 1 und 2 genannte Verzeichnis zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten für Unternehmen oder Einrichtungen, die 250 oder mehr Beschäftigte haben. Sie gilt darüber hinaus für Unternehmen oder Einrichtungen mit weniger als 250 Beschäftigten, wenn durch die Verarbeitung die Rechte und Freiheiten der betroffenen Personen gefährdet werden, die Verarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung besondere Datenkategorien gemäß § 11 bzw. personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des § 12 beinhaltet.

§ 38
Aufgaben des betrieblichen Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann er sich in Zweifelsfällen an die Datenschutzaufsicht gem. §§ 42 ff. wenden. Er hat insbesondere

a) die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

b) den Verantwortlichen oder den Auftragsverarbeiter zu unterrichten und zu beraten,

c) die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen,

d) auf Anfrage des Verantwortlichen oder des Auftragsverarbeiters diesen bei der Durchführung einer Datenschutz-Folgenabschätzung zu beraten und bei der Überprüfung, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung erfolgt, zu unterstützen und

e) mit der Datenschutzaufsicht zusammenzuarbeiten.

§ 50
Haftung und Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen dieses Gesetz ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen die kirchliche Stelle als Verantwortlicher oder Auftragsverarbeiter.

[...]

(4) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(5) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten kirchlichen Stellen als Verantwortlicher oder Auftragsverarbeiter den Schaden verursacht hat, so haftet jede als Verantwortlicher für den gesamten Schaden.

(6) Mehrere Ersatzpflichtige haften als Gesamtschuldner im Sinne des Bürgerlichen Gesetzbuches.

[...]

§ 51
Geldbußen

(1) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen dieses Gesetzes, so kann die Datenschutzaufsicht eine Geldbuße verhängen.

(2) Die Datenschutzaufsicht stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Paragraphen für Verstöße gegen dieses Gesetz in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

[...]

(6) Gegen kirchliche Stellen im Sinne des § 3 Absatz 1, soweit sie im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind, werden keine Geldbußen verhängt; dies gilt nicht, soweit sie als Unternehmen am Wettbewerb teilnehmen.

[...]

Raum für Ihre Notizen

Weitere Praxishilfen:

01 Wichtige Schritte bis zum In-Kraft-Treten des KDG

02 Der Betriebliche Datenschutzbeauftragte 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 Schriftenreihe wird gemeinsam herausgegeben von

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

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

Diözesandatenschutzbeauftragter für die
nordrhein-westfälischen (Erz-)Diözesen

Diözesandatenschutzbeauftragter
für die bayerischen (Erz-)Diözesen

Gemeinsame Datenschutzstelle der (Erz-)Diözesen
Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stutt-
gart, Speyer und Trier