KDG-Praxishilfe 13

Datenschutzorganisation und Datenschutzmanagement

nach dem neuen Gesetz über den Kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 13

Datenschutzorganisation und Datenschutzmanagement nach dem 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 1.0 / 11.12.2017

Datenschutzorganisation und Datenschutz-management nach dem Kirchlichen Datenschutz-gesetz (KDG)

1. Entwicklung des kirchlichen Datenschutzes

Die Europäische Datenschutz-Grundverordnung (DS-GVO) und in Anlehnung an sie das KDG gehen in Ansatz und Text davon aus, dass der Datenschutz in den Mitgliedstaaten und den Religionsgesellschaften zweigleisig verankert wird:

- Den Verantwortlichen und den betrieblichen Datenschutzbeauftragten fällt die Aufgabe zu, den Datenschutz in den Dienststellen zu organisieren, d.h., die Voraussetzungen dafür zu schaffen, dass er in jeder Ebene frei von Beanstandungen der Datenschutzaufsicht funktionieren kann. In diesem Bereich wird das eigentliche Datenschutzmanagement geleistet, während die nachfolgend besprochene Datenschutzaufsicht lediglich Kontrollaufgaben wahrnimmt.
- Die Datenschutzaufsicht (Diözesandatenschutzbeauftragter) hat in diesem Zusammenhang ausschließlich die Aufgabe, die Rechtmäßigkeit der Datenverarbeitung durch die kirchlichen Dienststellen zu prüfen. Kommt sie dieser Aufgabe nicht hinreichend nach, ist die Gleichwertigkeit des kirchlichen Datenschutzes mit dem staatlichen – und damit im Ergebnis die kirchliche Selbstverwaltungsfreiheit – ernsthaft in Frage gestellt.

2. Organisation der kirchlichen Datenschutzaufsicht

Während es bis 2015 noch Standard in allen Diözesen mit Ausnahme der norddeutschen und bayerischen Diözesen war, dass für jede von ihnen ein eigener Diözesandatenschutzbeauftragte bestellt wurde und dass dieser nebenbei auch noch allgemeine juristische Aufgaben oder solche übernommen hat, die typischerweise jetzt den betrieblichen Datenschutzbeauftragten zugewiesen sind, erfolgte seit 2015 mit Blick auf das Urteil des Europäischen Gerichtshofes vom 09.03.2010 eine Konzentration im Bereich der Datenschutzaufsicht.

Es gibt nunmehr fünf Bereiche der Datenschutzaufsicht in Deutschland:

- Nord
- Ost
- Nordrhein-Westfalen
- Südwest
- Bayern

Die Bischöfe der betroffenen Diözesen haben jeweils einen gemeinsamen Diözesandatenschutzbeauftragten für die genannten Bereiche bestellt.

3. Trennung von Datenschutzaufsicht und Datenschutzmanagement

Dadurch, dass für beide Personen – den betrieblichen wie den Diözesandatenschutzbeauftragten - der Begriff „**Datenschutzbeauftragte**r“ gebraucht wird, kam und kommt es auch im kirchlichen Bereich vielfach zu Verwirrungen, die historisch bedingt sind: Bis 2003 hat zwar der Diözesandatenschutzbeauftragte auch die Organisation des Datenschutzes faktisch übernommen. Es wird aber in der Zukunft besonders wichtig, die Institutionen sauber auseinanderzuhalten, weil z. B. gerade auch das Fehlen von betrieblichen Datenschutzbeauftragten in ausreichender Zahl dazu führen könnte, dass die Verantwortlichen kirchlicher Dienststellen mit sehr empfindlichen Bußgeldern belegt werden (siehe § 51 KDG).

Im Hinblick auf die Organisation wird von vielen betroffenen Dienststellen das Argument gebracht, dass die Datenschutzaufsicht ja ohnehin vorhanden sein müsse und dass man bei ihr – vor allem im Hinblick auf die Zentralisierung von Aufgaben in mehreren Diözesen – am besten auch das Datenschutzmanagement unterbringen sollte. Dies erspare vor allem bei einer Zuständigkeit für mehrere Diözesen den Aufbau einer weiteren Zentralbehörde und sei jedenfalls kostengünstiger als die bezeichnete Alternative.

Gegen diese Meinung ist allerdings einzuwenden, dass eine derartige Funktionsverteilung von der Europäischen Datenschutz-Grundverordnung nicht vorgenommen wird und dass die Doppelaufgabe Datenschutzmanagement und Datenschutzaufsicht deswegen dazu führen könnte, das gesamte Modell als mit der Verordnung nicht mehr in Einklang zu

sehen. Insbesondere muss erkannt werden, dass die Datenschutzaufsicht keine vernünftige Kontrollfunktion in einem Bereich übernehmen kann, den sie selbst geregelt hat. Letztlich wird also nichts anderes übrigbleiben, als eine parallele Datenschutz-Management-Organisation auf der Basis der Verantwortlichen unter starker Mitwirkung der betrieblichen Datenschutzbeauftragten zu schaffen.

4. Beteiligte des Datenschutzmanagements

Das KDG erlaubt in § 35 zwei grundsätzliche Modelle der betrieblichen Datenschutzbeauftragten.

Sie können entweder **Mitarbeiter des Verantwortlichen** sein oder als **externe Dienstleister** für die Einrichtung tätig werden. Gerade bei letzterem Modell wird klar, dass betriebliche Datenschutzbeauftragte einer Einrichtung auch mehrere natürliche Personen sein können. Das gilt entsprechend für die Benennung eines Mitarbeiters, weil das KDG nicht ausschließt, dass gleichzeitig auch Vertreter des betrieblichen Datenschutzbeauftragten benannt werden. Durch die Benennung muss lediglich klargestellt sein, wer im konkreten Fall die zuständige Ansprechperson ist.

Für das Datenschutzmanagement sind nach § 26 bis 28 KDG zwar in erster Linie die Verantwortlichen zuständig; sie werden jedoch in erheblichem Umfang von den betrieblichen Datenschutzbeauftragten durch Rat und Tat unterstützt. Zu beachten ist, dass in der verfassten Kirche die Mindestzahl von elf Mitarbeitern, die Daten verarbeiten, **weggefallen** ist.

5. Aufgaben des Datenschutzmanagements

Zu den Aufgaben des Datenschutzmanagements gehören unter anderem:

- Erfassung der Tatsachen, insbesondere der Schwachstellen
- Periodisch erneuerte Schwachstellenanalyse
- Erstellung eines Datenschutzkonzepts
- Erstellung von Verfahrensverzeichnissen

- Durchführung von Mitarbeiterschulungen und -fortbildungen
- Mitarbeitermotivation
- Planung des personellen Einsatzes
- Beteiligung an Zukunftsplanungen der Dienststelle
- Meldungen von Datenschutzverletzungen

Zum Schutz der gespeicherten Daten hat die Dienststelle nach Anweisung des Verantwortlichen diejenigen Maßnahmen zu ergreifen, die notwendig sind um Gefahren abzuwenden, aber auch im Verhältnis zur Bedeutung der Daten stehen (siehe § 26 KDG).

6. Datenschutzkonzept

Das Datenschutzkonzept sollte enthalten

- den zu betrachtenden Regelungsbereich
- eine kurze Beschreibung des IT-Systems
- die personenbezogenen Daten, einschließlich der rechtlichen Grundlage ihrer Erhebung, Speicherung bzw. Nutzung sowie des Zwecks der Erhebung
- eine Risikoanalyse, welche die denkbaren Schadszenarien und deren Eintrittswahrscheinlichkeit enthält sowie
- die kurze Beschreibung der getroffenen und unter Verhältnismäßigkeitsgesichtspunkten nicht getroffenen konkreten Maßnahmen

Das Vorhalten eines ausreichenden Datenschutzmanagements, z.B. in der Form einer ausreichenden Zahl betrieblicher Datenschutzbeauftragter, ist Gegenstand der Überprüfung durch die Aufsichtsbehörde. Reicht das personelle Engagement der Dienststelle nicht, muss die Aufsichtsbehörde zunächst durch Beanstandungen und dann gegebenenfalls durch Verhängung von Geldbußen dafür sorgen, dass ausreichende personelle Deckung geschaffen wird.

7. Gesetzestext §§ 26, 31 und 36 KDG (VDD Beschlussfassung vom 20.11.2017)

§ 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.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(4) Die Einhaltung eines nach dem EU-Recht zertifizierten Verfahrens kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen gemäß Absatz 1 nachzuweisen.

(5) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte um sicherzustellen, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach kirchlichem oder staatlichem Recht zur Verarbeitung verpflichtet.

§ 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.

§ 36
Benennung von betrieblichen Datenschutzbeauftragten

(1) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. a) benennen schriftlich einen betrieblichen Datenschutzbeauftragten.

(2) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. b) und c) benennen schriftlich einen betrieblichen Datenschutzbeauftragten, wenn

a) sich bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen,

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 besteht.

(3) Für mehrere kirchliche Stellen im Sinne des § 3 Absatz 1 kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer betrieblicher Datenschutzbeauftragter benannt werden.

(4) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des betrieblichen Datenschutzbeauftragten. Die Benennung von betrieblichen Datenschutzbeauftragten nach Absatz 1 ist der Datenschutzaufsicht anzuzeigen.

(5) Der betriebliche Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags oder einer sonstigen Vereinbarung erfüllen. Ist der betriebliche Datenschutzbeauftragte

Beschäftigter des Verantwortlichen, finden § 42 Absatz 1 Satz 1 2. Halbsatz und § 42 Absatz 1 Satz 2 entsprechende Anwendung.

(6) Zum betrieblichen Datenschutzbeauftragten darf nur benannt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

(7) Zum betrieblichen Datenschutzbeauftragten soll derjenige nicht benannt werden, der mit der Leitung der Datenverarbeitung beauftragt ist oder dem die Leitung der kirchlichen Stelle obliegt. Andere Aufgaben und Pflichten des Benannten dürfen im Übrigen nicht so umfangreich sein, dass der betriebliche Datenschutzbeauftragte seinen Aufgaben nach diesem Gesetz nicht umgehend nachkommen kann.

(8) Soweit keine Verpflichtung für die Benennung eines betrieblichen Datenschutzbeauftragten besteht, hat der Verantwortliche oder der Auftragsverarbeiter die Erfüllung der Aufgaben nach § 38 in anderer Weise sicherzustellen.

Weitere Praxishilfen:

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

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

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