KDG-Praxishilfe 1

Wichtige Schritte bis zum Inkrafttreten des KDG

nach dem neuen Gesetz über den kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 1

Wichtige Schritte bis zum Inkrafttreten des kirchlichen Datenschutzgesetzes (KDG)

Seite

1. Vorbemerkung 3
2. Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB) 4
3. Bestandsaufnahme aller durchgeführten Verarbeitungsprozesse 4
4. Prüfung der Rechtsgrundlagen 5
5. Besonderer Schutz der Daten von Kindern und Jugendlichen 5
6. Rechte der Betroffenen durch transparente Informationen unterstützen 6
7. Rechte der Betroffenen umsetzen..... 6
8. Die eigene Dokumentation im Bereich der Datenverarbeitung organisieren 7
9. Bestehende Verträge mit Auftragsverarbeitern überprüfen und anpassen 7
10. Möglichkeit zur Vornahme einer Datenschutz-Folgenabschätzung einrichten..... 8
11. Erweiterte Maßnahmen der Datenschutzaufsicht 9
12. Haftung und Schadensersatz..... 9
13. Gerichtliche Überprüfung 10

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 norddeutschen (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 / 07.12.2017

Wichtige Schritte bis zum Inkrafttreten des kirchlichen Datenschutzgesetzes (KDG)

1. Vorbemerkung

Durch die Europäische Datenschutzgrundverordnung (DS-GVO) wird das Datenschutzrecht innerhalb der Europäischen Union vereinheitlicht. Dies ist ein entscheidender Schritt, um das fundamentale Recht aller Bürger auf Erhaltung ihrer Intimsphäre auch im digitalen Zeitalter zu gewährleisten. Die Kirchen, die sich dem Wohl der Menschen in besonderer Weise verpflichtet fühlen, werden sich diesem Anliegen anschließen. Der Art. 91 DS-GVO gibt den Religionsgesellschaften die Möglichkeit für ihre Einrichtungen eigene Regelungen zu erstellen, die aber mit der Grundverordnung in Einklang zu bringen sind. In dieser Weise soll auch bei uns die Einheitlichkeit mit dem europäischen Recht hergestellt werden. Aus diesem Grunde wurde eine neue Regelung zum Datenschutz vorbereitet, über welche in der Herbstversammlung 2017 des Verbandes der Deutschen Diözesen (VDD) entschieden wurde. Das neue Kirchliche Datenschutzgesetz (KDG) wird die bisher geltende Anordnung über den kirchlichen Datenschutz (KDO) ablösen. Diese Vorschrift wird am 24. Mai 2018 in Kraft treten, also noch vor dem 25. Mai 2018, dem Zeitpunkt, zu dem die DS-GVO im gesamten europäischen Raum Rechtsgültigkeit erlangt.

Hierdurch werden die Rechte der Betroffenen wesentlich gestärkt und durch die Einrichtung einer erweiterten Datenschutzaufsicht im Rahmen der Regelungen des Kapitel VI DS-GVO abgesichert. Es wird eine Fülle von Änderungen geben, auf die sich unsere Dienststellen und Einrichtungen schon jetzt vorbereiten sollten. Die anschließend wiedergegebenen Empfehlungen sollten aus diesem Grund schon jetzt in Angriff genommen werden. Dabei wird in dieser Darstellung der aktuelle Entwurf für das geplante Gesetz zugrunde gelegt. Dies erfolgt unter dem Vorbehalt, dass sich durch Beschluss der Bischofskonferenz noch einzelne Bestimmungen geändert werden können, die sich aber auch in diesem Fall ebenfalls im Einklang mit der DS-GVO befinden müssen.

Diese Praxishilfe will für Dienststellen und Einrichtungen Anregungen geben, um sich auf das neue Gesetz vorbereiten zu können.

2. Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB)

Künftig müssen alle kirchlichen Diözesen, Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbände **unabhängig von der Zahl ihrer Mitarbeiter** einen eigenen betrieblichen Datenschutzbeauftragten (bDSB) bestellen. Dies sieht der § 36 Abs. 1 Satz 1 KDG i.V.m. § 3 Abs. 1 lit. a) KDG vor. Andere Einrichtungen, wie die der Caritas müssen nach § 36 Satz 2 ebenfalls einen betrieblichen Datenschutzbeauftragten bestellen, wenn ihre Kerntätigkeit in der Verarbeitung besonderer Kategorien von personenbezogenen Daten (§§ 4 Zi. 2, 11 KDG) besteht. Das gilt vor allem für Einrichtungen, die die gesetzliche Verschwiegenheitspflicht zu wahren haben. Schließlich ist ein bDSB zu ernennen, wenn **mindestens zehn Personen** mit der Verarbeitung personenbezogener Informationen beschäftigt sind. Im Unterschied zu der noch geltenden Regelung in § 20 Abs. 2 KDO ist hier die Einschränkung auf die Verarbeitung in elektronischen Medien entfallen. Auch Personen, die nur mit Aktenverwaltung betraut sind, müssen hier mitgerechnet werden. Und die Verpflichtung gilt ebenfalls bei zehn Mitarbeitern und nicht wie bisher bei der Zahl elf. Die Formulierung „mehr als zehn Personen“ ist durch „mindestens zehn Personen“ ersetzt worden. Daher müssen sämtliche Schulen und Kindergärten, mit zehn oder mehr pädagogischen Mitarbeitern ebenfalls einen bDSB bestellen! Eine „Kann“-Vorschrift besteht insoweit nicht mehr.

Durch diese Bestimmungen wird die Zweigleisigkeit der Datenschutzorganisation durch betriebsinterne Beauftragte einerseits und der Aufsicht des Diözesandatenschutzbeauftragten andererseits, sichergestellt. Es sollte daher geprüft werden:

- Ist bereits zum gegenwärtigen Zeitpunkt ein betrieblichen Datenschutztbeauftragten ernannt worden?
- Falls nicht: werden Vorbereitungen zu seiner künftigen Bestellung getroffen?
- Gibt es Absprachen, mit anderen Einrichtungen zur Bestellung eines gemeinsamen Datenschutzbeauftragten?
- Wie kann und soll die Fachkunde des Beauftragten sichergestellt werden?

3. Bestandsaufnahme aller durchgeführten Verarbeitungsprozesse

Nach § 3a KDO war schon bisher ein Verfahrensverzeichnis aller automatisierten Datenverarbeitungsprozesse erforderlich. Diese Verpflichtung wird auch nach dem neuen KDG für alle Einrichtungen mit 250 oder mehr Beschäftigten bestehen und ebenso für kleinere Einrichtungen, wenn ihre Verarbeitung die Rechte der betroffenen Personen gefährdet, die Verarbeitung nicht nur gelegentlich erfolgt oder besondere Datenkategorien beinhaltet (§ 31 Abs. 1 bis 5 KDG).

Daher sollte bereits jetzt überlegt werden:

- Muss ein Verzeichnis der Verarbeitungstätigkeiten führen?
- Liegen schon Verfahrensverzeichnisse nach § 3a KDO vor, die zur Grundlage der Verzeichnisse der Verarbeitungstätigkeiten nach KDG gemacht werden können?
- Sind die vorhandenen Verzeichnisse noch aktuell?

4. Prüfung der Rechtsgrundlagen

Schon bisher darf eine Datenverarbeitung **nur dann erfolgen**, wenn kirchliche oder staatliche Rechtsvorschriften sie erlauben oder anordnen oder die betroffene Person in die Verarbeitung für einen oder mehrere Zwecke eingewilligt hat. Dieser Grundsatz wird von § 6 KDG übernommen und darüber hinaus werden noch folgende Fälle der Zulässigkeit ausdrücklich benannt:

- Die Erfüllung eines Vertrages oder Vorvertrages, an dem die betroffene Person beteiligt ist.
- Die Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt.
- Erforderlichkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten.
- Erforderlichkeit für die Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liegt oder für die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde.
- Die Verarbeitung ist zur Wahrung der Interessen des Verantwortlichen oder eines Dritten erforderlich, soweit dabei nicht die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Güterabwägung).

Die aktuell durchgeführten Verarbeitungsprozesse müssen daher rechtzeitig, vor Inkrafttreten des KDG darauf geprüft werden, welche Rechtsgrundlage für sie besteht.

5. Besonderer Schutz der Daten von Kindern und Jugendlichen

Das neue Recht schützt besonders Minderjährige vor den **Risiken elektronischer Datenverarbeitung**. Grundsätzlich ist die Datenverarbeitung bei Anmeldungen oder Bestellungen im Internet, auch bei Erwachsenen nur mit der Einwilligungserklärung der Betroffenen erlaubt. Eine solche Erklärung, so bestimmt § 8 Abs. 8 KDG, kann aber künftig nur von Personen abgegeben werden, die das 16. Lebensjahr vollendet haben. In allen anderen Fällen, ist die Einwilligung der Personensorgeberechtigten erforderlich. Daher haben alle Einrichtungen, die elektronische Angebote bereitstellen, unter Berücksichtigung der zur Verfügung stehenden Technik, alle Anstrengungen zu unternehmen, um dies zu gewährleisten.

Diese Verpflichtung gilt unabhängig davon, ob der betreffende junge Mensch zivilrechtlich im Stande ist, wirksame Verträge selbst abzuschließen. Also auch bei der Bestellung einer CD für 10 €, die im Rahmen der Taschengeldregelung rechtswirksam sein mag, ist die Datenverarbeitung bei elektronischer Bestellung nur mit Einwilligung der Sorgeberechtigten wirksam. Lediglich für **kostenfreie** Beratungsangebote einer kirchlichen Stelle ist die Einwilligung der Eltern in die Datenverarbeitung nicht erforderlich, wenn das Kind bereits 13 Jahre alt ist. Hierdurch soll gewährleistet werden, dass eine pädagogische oder psychologische Beratung auch dann erfolgen kann, wenn sie sich auf Schwierigkeiten mit dem Elternhaus, bezieht.
Alle kirchlichen Angebote sind schon jetzt in dieser Hinsicht zu überprüfen und geeignete technische Maßnahmen zur Feststellung des Alters der betroffenen Personen vorzunehmen.

6. Rechte der Betroffenen durch transparente Informationen unterstützen

Betroffene sind künftig in transparenter Weise, das heißt in einer einfachen und klaren Sprache über die Verarbeitung ihrer Daten präzise, verständlich und in leicht zugänglicher Form zu informieren (§ 14 Abs. 1 bis 6 KDG). Dabei können auch standardisierte Bildsymbole verwendet werden. Besonderes Augenmerk ist dabei auf Informationen an Minderjährige zu legen. Auch für sie muss eine Verständlichkeit erreicht werden. Der Umfang der Informationspflicht soll durch § 15 KDG bei unmittelbarer Datenerhebung und § 16 KDG bei mittelbarer Datenerhebung in weitem Umfange präzisiert werden. Die kirchlichen Einrichtungen sollten daher frühzeitig die fachlichen und technischen Vorraussetzungen schaffen, um die gesetzlichen Anforderungen umzusetzen.

7. Rechte der Betroffenen umsetzen

Die Rechte der Betroffenen werden durch die Vorschriften der §§ 17 bis 25 KDG in Übereinstimmung mit der DS-GVO ausgeweitet. Das gilt vor allem für das Recht auf Löschung, § 19 KDG und das Recht auf Datenübertragbarkeit, § 22 KDG. So ist eine Löschung der Betroffenendaten auch dann vorzunehmen, wenn die Einwilligung zu ihrer Verarbeitung widerrufen wird und keine andere Rechtsgrundlage für ihre weitere Verwendung besteht. Darüber hinaus besteht ein Widerspruchsrecht bei der Verarbeitung von Daten, die zum Zwecke der Direktwerbung oder für Profiling verwendet werden, § 23 KDG. Neu ist das Recht auf Datenübertragbarkeit in elektronischen Verfahren, bei dem die Person das Recht hat, zu verlangen, dass ihre Daten von einem Verantwortlichen an einen anderen

Verantwortlichen übermittelt werden. Das dürfte vor allem in den Fällen von Bedeutung sein, bei denen der Anbieter von Dienstleistungen gewechselt werden soll. Es muss schon jetzt sichergestellt werden, dass diese Änderungen schon zum Zeitpunkt des Inkrafttretens des KDG umgesetzt werden können.

8. Die eigene Dokumentation im Bereich der Datenverarbeitung organisieren

Das KDG sieht an mehreren Stellen Dokumentationspflichten für die datenverarbeitenden Stellen vor:

- § 31 KDG verlangt, dass ein Verzeichnis aller Verarbeitungstätigkeiten geführt wird.
- Bei Auftragsverarbeitung ist nach § 29 Abs. 4 lit. c) in Verbindung mit § 26 Abs. 1 lt. d) KDG ein Verfahren, zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen organisatorischen und technischen Maßnahmen durchzuführen und zu ihrem Nachweis zu dokumentieren.
- Nach § 33 KDG sind Datenschutzvorfälle an die Datenschutzaufsicht unverzüglich zu melden und nach Absatz 5 zu dokumentieren.
- Nach § 40 Abs. 2 KDG sind Übermittlungen in Drittländer, die ohne einen Angemessenheitsbeschluss der Europäischen Kommission erfolgen, aber bei geeigneten Garantien vorgenommen werden, zu dokumentieren.

Bereits jetzt sollten diese Pflichten in die Organisation der Dienststelle einbezogen und dabei die Fragen, wer für die Führung dieser Verzeichnisse verantwortlich sein soll, in welcher Form sie geführt werden, wo sie verwahrt werden sollen und wer für die Meldungen an die Datenschutzaufsicht die Verantwortung trägt, entschieden werden.

9. Bestehende Verträge mit Auftragsverarbeitern überprüfen und anpassen

Bestehende Verträge zur Auftragsverarbeitung sind zu überprüfen und gegebenenfalls an die neue Vorschrift des § 29 KDG anzupassen. Zu den bisherigen Verpflichtungen kommen folgende hinzu:

- Die Verpflichtung des Auftragnehmers, seine Mitarbeiter auf das Datengeheimnis zu verpflichten.
- Haftung des Auftragnehmers für Pflichtverletzungen durch Unterauftragsnehmer.

- Die Pflicht zur regelmäßigen Kontrolle über die Einhaltung der technischen und organisatorischen Maßnahmen des Auftragnehmers.
- Der Auftragnehmer ist nach § 31 Abs. 2 KDG vertraglich zu verpflichten, ein Verzeichnis aller Tätigkeiten zu erstellen, die für den Auftraggeber ausgeführt werden.

Nach der Übergangsbestimmung in § 57 Abs. 3 KDG gelten bereits bestehende Vereinbarungen zur Auftragsdatenverarbeitung nach § 8 KDO fort, sie sind bis zum 31.12.2019 an die Vorgaben des KDG anzupassen. Neue Verträge zur Auftragsverarbeitung sind ab dem 24. Mai 2018 nach § 29 KDG abzuschließen.

10. Möglichkeit zur Vornahme einer Datenschutz-Folgenabschätzung einrichten

Die Vorschrift des § 35 KDG verpflichtet zur Vornahme einer Datenschutz-Folgenabschätzung durch die verantwortliche Stelle, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Das Risiko kann sich ergeben aus der Art, dem Umfang, der Umstände und der Zwecke der Verarbeitung. Sie ist nach § 35 Absatz 4 KDG insbesondere in folgenden Fällen erforderlich:

- Bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf einer automatisierten Verarbeitung, einschließlich Profiling, gründet.
- Bei einer umfangreichen Verarbeitung besonderer Kategorien von Daten nach § 11 Abs. 1 KDG oder Daten strafrechtlicher Verurteilungen.
- Bei der systematischen und umfangreichen Überwachung öffentlich zugänglicher Bereiche.
- Nach § 35 Absatz 5 KDG kann der Diözesandatenschutzbeauftragte zudem eine Liste von Verarbeitungsvorgängen erstellen und veröffentlichen, für die **in jedem Fall** eine Folgenabschätzung durchzuführen ist. Dabei soll er sich an den Listen der Aufsichtsbehörden aus Bund und Ländern orientieren.

Nach § 35 Absatz 7 KDG umfasst die Datenschutz-Folgenabschätzung folgende Punkte:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge, einschließlich ihrer Zwecke.
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf die Erreichung des Zwecks.

- Eine Bewertung der Risiken für die betroffenen Personen.
- Eine Darstellung der geplanten Abhilfemaßnahmen zur Bewältigung dieser Risiken. Dabei sind Garantien, Sicherheitsvorkehrungen und Schutzverfahren anzugeben, die den Nachweis zur Einhaltung dieses Gesetzes erbringen.

Der betriebliche Datenschutzbeauftragte ist hieran zu beteiligen. Kommt er zu dem Ergebnis, dass eine Datenschutz-Folgenabschätzung nicht ohne die Hinzuziehung der Datenschutzaufsicht erfolgen kann, ist der zuständige Diözesandatenschutzbeauftragte von ihm einzuschalten. Die bisherige Vorabkontrolle nach § 3 Abs. 5 KDO wird durch das neue Recht entfallen.

11. Erweiterte Maßnahmen der Datenschutzaufsicht

Bei der Feststellung von Verstößen gegen das KDG kann der Diözesandatenschutzbeauftragte nach § 47 KDG

- diese beanstanden und eine Frist zur Behebung gegenüber dem Verantwortlichen setzen (Abs. 1);
- bei Nichtbehebung der Mängel die Aufsicht führende Stelle verständigen und sie zu einer Stellungnahme auffordern (Abs. 3);
- Anordnungen erlassen, die geeignet sind einen rechtmäßigen Zustand wiederherzustellen oder Gefahren für die Betroffenen abzuwehren (Abs. 5), insbesondere auch Verarbeitungen zu verbieten (3 47 Abs. 5 lit. c)
- **Geldbußen zu verhängen** (Abs. 6). **Sie müssen im Einzelfall wirksam, verhältnismäßig und abschreckend sein** (§ 51 Abs. 1 KDG) **und können bis zu 500.000 Euro betragen** (§ 51 Abs. 4 KDG).

12. Haftung und Schadensersatz

Erstmals wird nunmehr in § 50 KDG die zivilrechtliche Haftung für das Entstehen materieller und immaterieller Schäden zu Lasten der betroffenen Person geregelt. Eine betragsmäßige Haftungsbeschränkung ist dabei nicht vorgesehen. Mehrere Ersatzpflichtige haften als Gesamtschuldner. Dem Betroffenen kommt außerdem zugute, dass eine Feststellung der Aufsichtsbehörde, eine Datenschutzverletzung habe objektiv vorgelegen, im Prozess vor den Zivilgerichten bindend ist (§ 47 Abs. 2 KDG).

13. Gerichtliche Überprüfung

Erstmals wurde auch die Möglichkeit eines gerichtlichen Rechtsbehelfs gegen eine Entscheidung der Datenschutzaufsicht oder gegen den Verantwortlichen geschaffen. Die Vorschrift des § 49 KDG bestimmt, dass hierfür ein kirchliches Gericht in Datenschutzangelegenheiten zuständig ist. Insoweit wird eine „Ordnung für die kirchlichen Gerichte in Datenschutzangelegenheiten (KDSGO) geschaffen werden.

Bitte merken:
Entspricht eine Datenverarbeitung zum Stichtag des Inkrafttretens des KDG nicht den Anforderungen und Festlegungen dieses Gesetzes, dann ist das Verfahren zumindest teilweise rechtswidrig und kann beanstandet und mit weiteren Maßnahmen, auch Bußgeldern, belegt werden!

Weitere Praxishilfen:

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 Schriftenreihe 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

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