KDG-Praxishilfe 7

Transparenz- und Dokumentationspflichten

nach dem neuen Gesetz über den Kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 7

Transparenz- und Dokumentationspflichten 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 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 2.0/ 01.02.2018

Transparenz- und Dokumentationspflichten nach dem Kirchlichen Datenschutzgesetz (KDG)

Grundsatz der Transparenz

Zu den wichtigen Grundsätzen der Verarbeitung personenbezogener Daten gehört ein transparentes Verhalten gegenüber den Betroffenen! Im Erwägungsgrund 39 der Datenschutzgrundverordnung wird hierzu festgestellt:

> *„Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der **Grundsatz der Transparenz** setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind.[...]“*

In Art. 5 der DS-GVO werden die Grundsätze für eine personenbezogene Datenverarbeitung verbindlich festgeschrieben. An erster Stelle wird in Art. 5 Abs. 1 lit. a) DS-GVO gefordert, dass „Personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz).“ In § 7 des KDG ist diese Bestimmung **weitestgehend** übernommen worden. Dabei wurden nur die Formulierung „nach Treu und Glauben“ und die in Klammern gesetzten Stichworte der DS-GVO im KDG entfernt. Um Missverständnissen vorzubeugen, muss zu diesen Änderungen etwas gesagt werden.

Der Begriff von Treu und Glauben könnte im kirchlichen Kontext zu unzutreffenden Auslegungen führen. Das Merkmal „Treu und Glauben“ im Sinne der DS-GVO ist nicht gleichzusetzen mit dem Begriffsverständnis von „Treu und Glauben“ im Sinne der deutschen Rechtstradition. Der Grundsatz ist als im Privatrechtsverkehr „notwendiges Korrektiv der prinzipiellen Freiheit des Einzelnen“ anzusehen. Auf das Verhältnis zwischen Staat und Bürger, welches auch in Datenverarbeitungsvorgängen geprägt ist, findet es als solches keine Anwendung. Es geht eher um einen „fair-use“-Ansatz wie er beispielsweise bei geistigen Schutzrechten im Common-Law bekannt ist.

In der englischen Übersetzung der DS-GVO wird an dieser Stelle der Begriff „Fairness“ eingesetzt, der im Prinzip dem gleichen Grundgedanken folgt. Man hat offensichtlich diesen Begriff im Text des KDG entfallen lassen, weil er üblicherweise nicht im Verwaltungsrecht verwendet wird. Das kann aber nichts daran ändern, dass auch von kirchlichen Datenverarbeitern erwartet wird, dass sie sich gegenüber den Betroffenen nach Treu und Glauben und somit fair verhalten.

Ein „faires“ Verhalten im Sinne der DS-GVO liegt nur dann vor, wenn alle Beteiligten über den jeweiligen Geschäftszweck, die Art und Weise, wie er herbeigeführt werden soll, die hieran Beteiligten und die Einbeziehung Dritter informiert sind. Bei der Verarbeitung personenbezogener Daten für Leistungen, die häufig von großen Anbietern angeboten werden, ist das nicht selbstverständlich der Fall. Hinzu kommt, dass viele Servicedienste zudem umsonst angeboten werden, wofür der Kunde allerdings regelmäßig „mit seinen Daten bezahlt“. Durch die Regelungen in § 14 KDG wird deshalb eine umfassende Informationspflicht des Verantwortlichen gegenüber dem Betroffenen verordnet. Im Einzelnen sind hiervon umfasst:

- Die Informationen bei unmittelbarer Datenerhebung nach § 15 KDG
- Die Informationen bei mittelbarer Datenerhebung nach § 16 KDG
- Alle Mitteilungen zum Auskunftsrecht der betroffenen Person nach § 17 KDG
- Die Mitteilung über eine vorgenommene Berichtigung - §§ 18, 21 Abs. 2 KDG
- Die Mitteilung über die Durchführung einer Löschung oder Sperrung der Daten - §§ 19 Abs. 1, 21 Abs. 2 KDG
- Die Mitteilung über die Einschränkung der Verarbeitung - §§ 20, 21 Abs. 2 KDG
- Zum Zwecke der Datenübertragbarkeit die Zurverfügungstellung der Daten in einem maschinenlesbaren Format nach § 22 Abs. 1 KDG
- Der Hinweis auf das Widerspruchsrecht nach § 23 Abs. 4 KDG
- Die Darlegung einer nach § 24 Abs. 2 lit. a) und c) vorgenommenen Entscheidung über eine automatisierte Datenverarbeitung (§ 24 Abs. 3 KDG)
- Benachrichtigung über eine Verletzung des Betroffenenschutzes, wenn dies ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (§ 34 Abs. 1, 2 KDG)

Wichtig ist hierbei, dass nicht nur die Informationen über die Daten, die bei dem Betroffenen selbst oder bei Dritten erhoben wurden, sondern auch Informationen über die weitere Verwendung erfolgen. Hierzu gehören alle Veränderungen des Datenbestandes durch Löschung, Sperrung und Einschränkung ihrer Verarbeitung. Auch der berechtigte Nutzerwechsel durch Vornahme der Übertragung der Daten auf einen anderen Verantwortlichen

wird an dieser Stelle mit erfasst.

Neu ist auch die Form des Vorliegens der Informationen. Der § 14 Abs. 1 KDG legt hierzu in Übereinstimmung mit Art. 12 Abs. 1 DS-GVO fest, dass die Übermittlung

- in präziser
- transparenter
- verständlicher
- leicht zugänglicher Form
- in einer klaren und einfachen Sprache
- gegebenenfalls auch durch Verwendung standardisierter Bildsymbole

zu erfolgen hat. Dabei ist auch in besonderer Weise auf die Situation Minderjähriger Rücksicht zu nehmen und speziell an sie gerichtete Informationen in entsprechender Weise zu gestalten.

Die Information ist in der Regel schriftlich, gegebenenfalls auch elektronisch (siehe hierzu: § 22 Abs. 1 KDG Recht auf Datenübertragbarkeit) oder in anderer Form vorzunehmen. Die Vorschrift wird sich in vielen Bereichen auswirken. So wird zum Beispiel zu überprüfen sein, ob die Datenschutzerklärung auf einer Webseite diesen Anforderungen genügt.

Dokumentationspflichten

Im Kirchlichen Datenschutzgesetz sind an verschiedenen Stellen Dokumentationspflichten des Verantwortlichen aber auch des Auftragsverarbeiters geregelt.

§ 31 KDG – Verzeichnis von Verarbeitungstätigkeiten

An erster Stelle ist das Verzeichnis **aller** Verarbeitungstätigkeiten nach § 31 Abs. 1 KDG von dem Verantwortlichen zu erstellen. Dabei sind alle Angaben aus dem § 31 Abs. 1 lit. a) bis h) zu berücksichtigen. In Bezug genommen werden hier nicht allein die elektronischen Verfahren, sondern jede Verarbeitung im Sinne der Begriffsbestimmung des § 4 Nr. 3 KDG. Hierzu gehört auch jede systematische Datenverarbeitung in Akten, auf Karteikarten oder ähnlichen Medien. Betroffen sind hiervon alle Einrichtungen, die 250 oder mehr Beschäftigte haben und auch kleinere Einheiten, wenn die Verarbeitung von Daten bei ihnen nicht nur gelegentlich erfolgt oder besondere Kategorien von Daten nach § 4 Nr. 2 und § 11 KDG verarbeitet werden.

Auch der **Auftragsverarbeiter** wird durch § 31 Abs. 2 KDG in Anspruch genommen. Auch er hat ein Verzeichnis der Auftragstätigkeiten zu erstellen und hierbei die Angaben nach

§ 31 Abs. 2 lit. a) bis d) KDG zu machen. Die Verzeichnisse sind schriftlich zu führen (§31 Abs. 3 KDG) und dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen (§ 31 Abs. 4 KDG). Auf Anforderung sind sie auch der Aufsichtsbehörde zur Verfügung zu stellen. Genauere Informationen können der Praxishilfe 5 „Das Verzeichnis der Verarbeitungstätigkeiten nach dem KDG“ entnommen werden.

§ 35 KDG – Datenschutz-Folgenabschätzung

In festgelegten Fällen ist die Durchführung einer Datenschutzfolgenabschätzung erforderlich. Die Einzelheiten hierzu werden in der Praxishilfe 11 „Datenschutz-Folgenabschätzung nach dem KDG“ dargestellt, so dass hier darauf verwiesen werden kann.

§ 29 KDG – Verarbeitung personenbezogener Daten im Auftrag

Die Verarbeitung erfolgt nach § 29 Abs. 3 KDG auf Grund eines Vertrages mit dem Auftragsverarbeiter, der schriftlich abzufassen ist (§ 29 Abs. 9 KDG). Inhaltlich sind dabei alle Anforderungen des § 29 Abs. 4 lit. a) bis h) KDG zu berücksichtigen. Die Einzelheiten können der Praxishilfe 4 „Auftragsdatenverarbeitung nach dem KDG“ entnommen werden. Der Vertrag ist auf Anforderung der Datenschutzaufsicht nach § 44 Abs. 2 lit. b) KDG zur Verfügung zu stellen.

§ 33 KDG - Meldung an die Datenschutzaufsicht

Das neue KDG verpflichtet die Verantwortlichen nach § 33 Abs. 1 KDG zur unverzüglichen Meldung von Datenschutzverletzungen, die eine Beeinträchtigung der Rechte und Freiheiten natürlicher Personen darstellen. Eine Verzögerung stellt es dabei dar, wenn die Nachricht nicht innerhalb von 72 Stunden nach Kenntniserlangung an die Aufsichtsbehörde übermittelt wird. Inhaltlich erstreckt sich die Meldung auf die in § 33 Abs. 3 lit. a) bis d) KDG genannten Punkte. § 33 Abs. 5 KDG legt fest, dass die datenschutzrechtlichen Verletzungen und alle mit ihr in Zusammenhang stehenden Tatsachen zu dokumentieren sind. Diese Aufzeichnung muss der Datenschutzaufsicht eine Überprüfung über die Einhaltung der Bestimmungen nach § 33 Abs. 1 - 4 KDG ermöglichen.

Der Auftragsverarbeiter ist nach § 33 Abs. 2 KDG verpflichtet, Datenschutzverletzungen dem Verantwortlichen zu melden. Dieser hat sie im Falle des § 33 Abs. 1 KDG an die Datenschutzaufsicht weiterzugeben.

Die hier wiedergegebene Verpflichtung ist neu geschaffen worden. Daher wurde zu diesem Thema auch eine eigenständige Praxishilfe verfasst. Bitte beachten Sie daher die Praxishilfe 10 „Umgang mit Datenpannen nach dem KDG“.

Gesetzestext von §§ 7, 14, 29, 33 und 35 KDG (VDD Beschluss-fassung vom 20.11.2017)

§ 7
Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen
   a) auf rechtmäßige und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
   b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
   c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein; insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und der Aufwand nicht außer Verhältnis zum angestrebten Schutzzweck steht;
   d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
   e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
   f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

(2) Der Verantwortliche ist für die Einhaltung der Grundsätze des Absatz 1 verantwortlich und muss dies nachweisen können.

§ 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.

(2) Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den §§ 17 bis 24. In den Fällen des § 13 Absatz 2 darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den §§ 17 bis 24 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den §§ 17 bis 24 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei der Datenschutzaufsicht Beschwerde zu erheben oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Informationen gemäß den §§ 15 und 16 sowie alle Mitteilungen und Maßnahmen gemäß den §§ 17 bis 24 und 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche

a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder

b) sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(6) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den §§ 17 bis 23 stellt, so kann er unbeschadet des § 13 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

§29
Verarbeitung personenbezogener Daten im Auftrag

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieses Gesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem kirchlichen Recht, dem Recht der Europäischen Union oder dem Recht ihrer Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem

a) Gegenstand der Verarbeitung
b) Dauer der Verarbeitung,
c) Art und Zweck der Verarbeitung,
d) die Art der personenbezogenen Daten,
e) die Kategorien betroffener Personen und
f) die Pflichten und Rechte des Verantwortlichen

festgelegt sind.

(4) Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das kirchliche Recht, das Recht der Europäischen Union oder das Recht ihrer Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen kirchlichen Interesses verbietet;
b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen

Verschwiegenheitspflicht unterliegen;

c) alle gemäß § 26 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 5 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in den §§ 15 bis 25 genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 26, 33 bis 35 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem kirchlichen Recht oder dem Recht der Europäischen Union oder dem Recht ihrer Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Paragraphen niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen dieses Gesetz oder gegen andere kirchliche Datenschutzbestimmungen oder Datenschutzbestimmungen der Europäischen Union oder ihrer Mitgliedstaaten verstößt.

(5) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem kirchlichen Recht oder dem Recht der Union oder dem Recht des betreffenden Mitgliedstaats der Europäischen Union dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß den Absätzen 3 und 4 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieses Gesetzes erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(6) Die Einhaltung nach europäischem Recht genehmigter Verhaltensregeln oder eines geneh-

migten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 5 nachzuweisen.

(7) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3, 4 und 5 ganz oder teilweise auf den in den Absatz 8 genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter erteilten Zertifizierung sind.

(8) Die Datenschutzaufsicht kann Standardvertragsklauseln zur Regelung der in den Absätzen 3, 4 und 5 genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3, 4 und 5 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Maßgebend sind die Formvorschriften der §§ 126 ff. BGB.

(10) Ein Auftragsverarbeiter, der unter Verstoß gegen dieses Gesetz die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

(11) Der Auftragsverarbeiter darf die Daten nur innerhalb der Mitgliedsstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeiten. Abweichend von Satz 1 ist die Verarbeitung in Drittstaaten zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission gemäß § 40 Absatz 1 vorliegt oder wenn die Datenschutzaufsicht festgestellt hat, dass dort ein angemessenes Datenschutzniveau besteht.

(12) Die Absätze 1 bis 11 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 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 offenge-

legt 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.

§ 33

Meldung an die Datenschutzaufsicht

(1) Der Verantwortliche meldet der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. Erfolgt die Meldung nicht binnen 72 Stunden, nachdem die Verletzung des Schutzes personenbezogener Daten bekannt wurde, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese unverzüglich dem Verantwortlichen.

(3) Die Meldung gemäß Absatz 1 enthält insbesondere folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der möglichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nach Absatz 3 nicht zeitgleich bereitgestellt werden können, stellt der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Datenschutzaufsicht die Überprüfung der Einhaltung der Bestimmungen der Absätze 1 bis 4 ermöglichen.

§ 35
Datenschutz-Folgenabschätzung und vorherige Konsultation

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge

für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des betrieblichen Datenschutzbeauftragten ein, sofern ein solcher benannt wurde.

(3) Ist der Verantwortliche nach Anhörung des betrieblichen Datenschutzbeauftragten der Ansicht, dass ohne Hinzuziehung der Datenschutzaufsicht eine Datenschutz-Folgenabschätzung nicht möglich ist, kann er der Datenschutzaufsicht den Sachverhalt zur Stellungnahme vorlegen.

(4) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(5) Die Datenschutzaufsicht soll eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine Datenschutz-Folgenabschätzung gemäß Absatz 1 durchzuführen ist. Sie kann ferner eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

(6) Die Listen der Datenschutzaufsicht sollen sich an den Listen der Aufsichtsbehörden des Bundes und der Länder orientieren. Gegebenenfalls ist der Austausch mit staatlichen Aufsichtsbehörden zu suchen.

(7) Die Datenschutz-Folgenabschätzung umfasst insbesondere:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien,

Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass dieses Gesetz eingehalten wird.

(8) Der Verantwortliche holt gegebenenfalls die Stellungnahme der betroffenen Person zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder kirchlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(9) Falls die Verarbeitung auf einer Rechtsgrundlage im kirchlichen Recht, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 5 nicht.

(10) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

(11) Der Verantwortliche konsultiert vor der Verarbeitung die Datenschutzaufsicht, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hat, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Raum für Ihre Notizen

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

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

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