KDG-Praxishilfe 4

Auftragsverarbeitung

nach dem neuen Gesetz über den kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesandatenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 4

Auftragsverarbeitung 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 / 07.12.2017

Auftragsverarbeitung nach dem Kirchlichen Datenschutzgesetz (KDG)

Die Zulässigkeit einer Auftragsverarbeitung nach dem KDG

Geregelt ist die Auftragsverarbeitung künftig in § 29 KDG, der sich an die Bestimmung in Art. 28 der Datenschutzgrundverordnung (DS-GVO) anlehnt.

Wie bereits in der noch geltenden KDO wird weiterhin der Auftragnehmer nicht als „Dritter" bei der „Offenlegung" personenbezogener Daten (frühere Bezeichnung: „Datenübermittlung") angesehen. Nach der Definition des Begriffs in § 4 Nr. 12 KDG ist „Dritter" jede natürliche oder juristische Person, soweit es sich bei ihr nicht um den Betroffenen selbst, den Verantwortlichen oder einen von ihm eingeschalteten Auftragsverarbeiter handelt. Der Auftragsverarbeiter ist also insoweit privilegiert, als eine Offenlegung der Daten an ihn ohne Prüfschranken erfolgen kann. Der Dienstleister wird also im „Innenverhältnis" für den Verantwortlichen tätig. Diese Privilegierung ist nur bei der Einhaltung folgender wichtiger Bedingungen möglich.

Bedingungen für die Privilegierung

- Der Dienstleister muss hinreichende Garantien dafür bieten, dass die von ihm getroffenen technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung nur im Einklang mit den Bestimmungen des KDG durchgeführt wird und dass dabei der Schutz der Rechte der Betroffenen gewährleistet ist. Nur hierdurch kann zwischen den Beteiligten das notwendige Vertrauen gebildet werden, das erforderlich ist, um den Auftragnehmer im Innenverhältnis an der Verarbeitung der Daten zu beteiligen.

- Der Dienstleister darf weitere Anbieter im Rahmen eines Unterauftragsverhältnisses nur mit ausdrücklicher Zustimmung des Verantwortlichen beteiligen. Hierzu kann insoweit eine vorherige gesonderte oder allgemeine **schriftliche Genehmigung** erfolgen. Beabsichtigte Änderungen hieran, sind vorab dem Verantwortlichen mitzuteilen, was diesem die Möglichkeit verschafft, gegebenenfalls Einspruch zu erheben.

Der Verantwortliche muss den vollständigen Überblick darüber behalten, wo und bei wem die ihm anvertrauten Daten verarbeitet werden. In der Vereinbarung ist der Subunternehmer genau zu benennen.

- Die Hineinnahme in das Innenverhältnis darf, wie bisher, nur auf Grund eines **schriftlichen Vertrages** erfolgen, das den Auftragnehmer an den Auftraggeber bindet und in dem zumindest der Gegenstand, die Dauer, die Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind (§ 29 Abs. 3 KDG). Der Vertrag kann nach § 29 Abs. 9 KDG auch in einem elektronischen Format abgeschlossen werden. Dies erleichtert die Zusammenarbeit mit großen Anbietern. Dabei ist auch § 29 Abs. 12 KDG zu beachten. Die Verpflichtung zur vertraglichen Regelung gilt nach § 29 Abs. 13 KDG auch für Wartungen automatisierter Verfahren, soweit dabei auch ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (Wartungsverträge).

- Durch § 29 Abs. 4 lit. c) KDG neu geschaffen wurde die **vertragliche Verpflichtung** des Auftragnehmers alle nach § 26 KDG („Technische und organisatorische Maßnahmen“) erforderlichen Maßnahmen zu ergreifen. Hierbei sind das angemessene Schutzniveau und die Risiken für die Rechte und Freiheiten der betroffenen Personen zu ermitteln und in der Vereinbarung festzuhalten. Weiterhin wird ein Datenschutzkonzept erforderlich sein, das die Verarbeitung auf Basis des festgestellten Schutzniveaus im notwendigen Umfang sichert.

- Der Dienstnehmer ist darüber hinaus nach § 31 Abs. 2 KDG vertraglich zu verpflichten, ein Verzeichnis zu allen Kategorien der von ihm durchgeführten Tätigkeiten zu erstellen. Dieses muss er nach § 31 Abs. 4 KDG der Vorschrift dem vom Verantwortlichen bestellten betrieblichen Datenschutzbeauftragten und auf Anforderung auch dem Diözesandatenschutzbeauftragten als Leiter der Aufsichtsbehörde zur Verfügung stellen.

- Für den Fall, dass eine Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen durch andere Stellen vorgenommen wird, hat eine entsprechende Anwendung des § 29 Abs. 1 bis 11 KDG stattzufinden. Soweit dabei die Möglichkeit besteht, dass der Auftragsverarbeiter mit den gespeicherten personenbezogenen Daten in Kontakt kommt, kann eine Hereinnahme in das Innenverhältnis nur unter Anwendung der hier festgelegten Regeln erfolgen.

Verantwortlichkeiten und Pflichten des Auftragnehmers

Das KDG legt in Übereinstimmung mit der DS-GVO dem Auftragnehmer eine Reihe neuer Verantwortlichkeiten auf.

- **Unterstützung der Aufgabenerfüllung des Verantwortlichen.** Nach Möglichkeit soll der Auftragsverarbeiter durch technisch-organisatorische Maßnahmen dem Verantwortlichen helfen, seine Verpflichtungen der betroffenen Person gegenüber nach den Vorschriften der §§ 15 bis 25 KDG zu erfüllen - § 29 Abs. 4 lit. e) KDG.

- Weiterhin soll der Auftragnehmer den Verantwortlichen bei der Einhaltung der Pflichten aus §§ 26 und 33 bis 35 unterstützen - § 29 Abs. 4 lit. f) KDG.

- **Haftung gegenüber den Betroffenen.** Hält sich der Auftragsverarbeiter nicht an seine Verpflichtung, die Daten nur auf Grund der Weisung des Verantwortlichen zu verarbeiten, in dem er selbst die Zwecke und Mittel der Verarbeitung bestimmt, wird er nach § 29 Abs. 10 KDG zum Verantwortlichen für diese Datenverarbeitung. Als Konsequenz hieraus ergibt sich, dass er alle Rechte der Betroffenen erfüllen muss.

- Hierzu gehört insbesondere auch die **Schadensersatzpflicht** nach § 50 Abs. 1 KDG. Der Auftragnehmer wird an dieser Stelle ausdrücklich mit benannt. Er ist bei Verstößen sowohl zum Ersatz des materiellen, wie auch des immateriellen Schadens (Schmerzensgeld) verpflichtet. Wenn nicht ermittelt werden kann, ob der Schaden durch den Verantwortlichen oder den Auftragsverarbeiter verursacht worden ist, haften sie gemeinsam.

- Wenn eine Verletzung des Schutzes personenbezogener Daten bekannt wird, ist der Auftragsverarbeiter verpflichtet, diese unverzüglich dem Verantwortlichen zu melden (**Meldepflicht - § 33 Abs. 2 KDG**). Ist damit eine Gefahr für die Rechte und Freiheiten natürlicher Personen verbunden, so hat der Verantwortliche die Aufsichtsbehörde ebenso unverzüglich, spätestens jedoch nach 72 Stunden, hierüber zu informieren.

- Eine Verarbeitung der Daten darf nur innerhalb der Europäischen Union oder dem europäischen Wirtschaftsraum erfolgen - § 29 Abs. 11 KDG. Abweichungen hiervon sind nur möglich, wenn in Bezug auf das Drittland durch eine Datenschutzbehörde festgestellt worden ist, dass dort ein angemessenes Datenschutzniveau besteht.

- Verstößt ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen die Bestimmungen des KDG, kann auch gegen ihn einer **Geldbuße** nach § 51 Abs. 1 KDG verhängt werden.

Einwirkungsmöglichkeiten der Datenschutzbeauftragten

- Der Auftragsverarbeiter hat hinreichende Garantien zur Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten zu gewährleisten (§ 29 Abs.1). Hierbei kann nach § 29 Abs. 6 KDG als wichtiger Faktor die **„Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens“** nach § 29 Abs. 1 und 5 KDG berücksichtigt werden.

- Die Datenschutzaufsicht kann **Standardvertragsklauseln** für die abzuschließenden Verträge und die dabei zu beachtenden Regeln festlegen, § 29 Abs. 8 KDG. Sie können ganz oder teilweise zum Inhalt der Vereinbarungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemacht werden, § 29 Abs. 7 KDG. Ihre Verwendung erhöht die Sicherheit der Datenverarbeitung und erleichtert eine Prüfung des Verfahrens durch die Aufsichtsbehörde. Zudem haben Auftragsverarbeiter, die für eine große Zahl von Verantwortlichen tätig sind, auf dieser Basis die Möglichkeit, einheitliche Vertragsbedingungen zu schaffen, insbesondere dann, wenn sie auch Bestandteil einer erteilten Zertifizierung sind. Die Datenschutzaufsichten des Bundes und der Länder beabsichtigen künftig gemeinsam, unter Einschluss kirchlicher Diözesandatenschutzbeauftragter, allgemein anwendbare Standardvertragsklauseln für unterschiedliche Anwendungsbereiche zu entwickeln.

Gesetzestext von § 29, und §§ 26, 31 und 33 (VDD Beschlussfassung vom 20.11.2017)

§ 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;
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 genehmigten 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 bis 5 genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 bis 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 Mitgliedstaaten 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 selbst oder eine andere 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.

§ 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.

§ 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.

Weitere Praxishilfen:

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

02 Der Betriebliche Datenschutzbeauftragte nach dem KDG

03 Verantwortlichkeiten nach dem KDG

05 Der 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