Formulierungshilfe

Verarbeitung pbDaten bei vertragsärztlichen Leistungen durch Unternehmen

gemäß dem Gesetz über den kirchlichen Datenschutz (KDG)

Stand 04/2018

Konferenz der Diözesandatenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Formulierungshilfe

Erstellung von Verträgen über die Verarbeitung personenbezogener Daten bei vertragsärztlichen Leistungen durch beauftragte Unternehmen

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

Diese Formulierungshilfe der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands dient als Orientierungshilfe. Die konkrete Ausgestaltung ist an den jeweiligen Sachverhalt anzupassen und sollte daher Schritt für Schritt für den konkreten Anwendungsfall erstellt werden. Dieses Dokument kann dies vereinfachen, aber nicht ersetzen. Diese Formulierungshilfe stellt keine zivilrechtliche Beratung durch das KDSZ und keine Standardvertragsklauseln im Sinne von § 29 Abs. 8 KDG bzw. Art. 28 Abs. 8 DS-GVO dar. Insbesondere ist durch das KDSZ keine Prüfung nach den §§ 307ff. BGB vorgenommen worden.

Revision 0.1 / 04.05.2018

Formulierungshilfe
Erstellung von Verträgen über die Verarbeitung personenbezogener Daten bei vertragsärztlichen Leistungen durch beauftragte Unternehmen

Wichtige Hinweise vorab

Mit der Abrechnung ärztlicher Leistungen, die gegenüber Privatpatienten erbracht wurden, werden von den Kliniken heute allgemein Drittdienstleister, nämlich privatärztliche Verrechnungsstellen beauftragt. Rechtlich war dies bisher nur statthaft, wenn die Einwilligung des Patienten zu die-sem Abrechnungsverfahren vorlag. In der Regel wurde diese schon bei der Aufnahme durch eine Vereinbarung des Patientenvertrages eingeholt. Nach dem neuen KDG ist dies nicht mehr erforderlich. Unter den Begriffsbestimmungen des § 4 Nummer 12 wurde im Einklang mit der Datenschutzgrundverordnung festgelegt, dass der Auftragsverarbeiter kein „Dritter“ im datenschutzrechtlichen Sinne ist. Alle Personen und Stellen, die unter der Aufsicht des Verantwortlichen befugt sind, personenbezogene Daten zu verarbeiten, gelten somit als bei der Datenverarbeitung privilegierte „Insider“. Bei der Auftragsverarbeitung nach § 29 bleibt wie bisher die Verantwortung gegenüber den Patienten für eine ordnungsgemäße Datenverarbeitung allein beim Auftraggeber (Umkehrschluss aus § 29 Abs. 10, wonach der Auftragnehmer nur durch Verstoß gegen dieses Gesetz zum Verantwortlichen der betreffenden Datenverarbeitung wird.).

➔ **Es ist keine Einwilligungserklärung des (Privat-)Patienten zur Auftragsabrechnung erforderlich.**

Die privilegierte Stellung des Auftragsverarbeiters setzt aber voraus, dass von beiden Seiten die von §§ 29, 30 KDG bestimmten Regelungen vollständig eingehalten werden. Nur dann ist der Schutz des informationellen Selbstbestimmungsrechts des Patienten auch unter den Bedingungen der Auftragsverarbeitung zu gewährleisten.

➔ **Eine Auftragsverarbeitung ist daher nur bei der Erfüllung der gesetzlichen Anforderungen zulässig!**

Folgende Bestimmungen sind zu beachten:

§ 35 I, IV Datenschutz-Folgenabschätzung

Sie ist erforderlich nach Absatz 4 lit. b), weil in umfangreicher Weise besondere Kategorien personenbezogener Daten verarbeitet werden (Diagnose- und Behandlungsdaten nach ICD 10). Der Auftragsvorgang, insbesondere die vertraglichen Festlegungen mit dem Auftragnehmer sind bei der Einschätzung der Folgen und der Risiken für die Patientendaten von erheblicher Bedeutung. Dies gilt sowohl hinsichtlich der rechtlichen Behandlung der Daten, wie auch gerade für die technischen Maßnahmen zu ihrer Sicherung.

➔ **Eine Folgenabschätzung muss die Risiken einer Auftragsverarbeitung berücksichtigen.**

§ 29 Verarbeitung personenbezogener Daten im Auftrag

Die Erfüllung der gesetzlichen Forderungen ist nur durch Abschluss eines umfangreichen und alle Punkte berücksichtigenden Vertrages zwischen dem Krankenhaus und dem Auftragsverarbeiter zu erreichen (Absatz 3). Nach Absatz 7 können solche Verträge entweder individuell festgelegt und vereinbart werden, oder auch ganz oder teilweise auf Standardvertragsklauseln beruhen, die nach Absatz 8 von der Aufsichtsbehörde festgelegt worden sind[1]. Die Standardvertragsklauseln sind in diesem Fall wörtlich zu übernehmen[2].

➔ **Wahlmöglichkeit: Individuell ausgehandelter Vertrag oder festgelegte Standardvertragsklauseln**

In beiden Fällen sind nach Absatz 3 lit. a) bis f) zwingend benannten Regelungsgegenstände festzulegen:

- Der Gegenstand der Verarbeitung
- Die Dauer der Verarbeitung
- Die Art und der Zweck der Verarbeitung
- Die Art der personenbezogenen Daten

1 Dies wird in Erwägungsgrund 81 zur DS-GVO ausdrücklich klargestellt. Der Text des Erwägungsgrundes 81 ist in der Anlage am Ende des Dokuments vollständig wiedergegeben.
2 Der Erwägungsgrund 168 spricht insoweit vom „Erlass von Rechtsakten". Der Text des Erwägungsgrundes 168 ist in der Anlage am Ende des Dokuments vollständig wiedergegeben.

- Die Kategorien betroffener Personen
- Die Pflichten und Rechte des Verantwortlichen

Weiterhin hat der Auftragnehmer laut Abs. 4 lit. a) bis h) folgende Verpflichtungen vertraglich zu übernehmen:

- Er darf eine Verarbeitung in Drittländern nur dann vorzunehmen, wenn dies auf Grund einer dokumentierten Weisung des Auftraggebers erfolgt.
- Es dürfen von ihm nur befugte Personen zur Verarbeitung eingesetzt werden, die sich zur Vertraulichkeit verpflichtet haben oder einer besonderen Verschwiegenheitspflicht unterliegen.
- Er verpflichtet sich, alle nach § 26 KDG erforderlichen Maßnahmen zu ergreifen.
- Er darf weitere Auftragnehmer nur in Anspruch nehmen, wenn hierfür die schriftliche Genehmigung des Auftraggebers vorliegt (Abs. 2) und durch Vertrag mit dem weiteren Auftragnehmer sichergestellt ist, dass dieser die gleichen Verpflichtungen erfüllt, wie sie sich aus dem zugrunde liegenden Auftragsverhältnis ergeben (Abs. 5).
- Er verpflichtet sich, den verantwortlichen Auftraggeber bei allen Anträgen von betroffenen Personen nach §§ 15 bis 25 KDG zu unterstützen, soweit die Anträge seinen Tätigkeitsbereich betreffen.
- Er verpflichtet sich, den Auftraggeber bei der Verwirklichung technisch-organisatorischer Maßnahmen (§ 26), der Vornahme einer notwendigen Folgenabschätzung (§ 35) und der Meldung von Datenschutzverstößen an die Aufsicht (§ 33) und der Benachrichtigung von Betroffenen hierüber (§ 34) zu unterstützen, soweit es seinen Aufgabenbereich betrifft.
- Er muss die Daten nach Wahl des Auftraggebers löschen oder zurückgeben, wenn die Erbringung der Verarbeitungsleistungen abgeschlossen sind.
- Er verpflichtet sich, dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der niedergelegten Pflichten zur Verfügung zu stellen und Prüfungen und Inspektionen durch den Auftraggeber zu ermöglichen und zu unterstützen.
- Er verpflichtet sich, den Auftraggeber zu informieren, wenn er der Meinung ist, dass eine ihm erteilte Weisung gegen Datenschutzbestimmungen verstößt.

➔ **Die genannten Verpflichtungen müssen durch entsprechende Bestimmungen des Vertrages verbindlich zwischen den Vertragspartnern festgelegt werden.**

§ 30 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede ihm unterstellte Person, die Zugang zu den personenbezogenen Daten hat, dürfen diese Daten nur nach der Weisung des Verantwortlichen verarbeiten.

§ 31 Absatz 2 Verzeichnis von Verarbeitungstätigkeiten

Der Auftragsverarbeiter ist vertraglich zu verpflichten, ein Verzeichnis der Verarbeitungstätigkeiten über die von ihm durchgeführten Arbeiten, zu erstellen. Die Vorschrift des KDG legt dies noch einmal ausdrücklich fest, obwohl sich diese Verpflichtung schon daraus ergibt, dass der Auftragsverarbeiter nicht als Dritter, sondern als interner Datenverarbeiter angesehen wird (so § 4 Ziffer 14). Diese Privilegierung setzt allerdings voraus, dass er sich hinsichtlich der von ihm übernommenen Arbeiten, in gleichem Maße an der ordnungsgemäßen Organisation und Sicherung der Datenverarbeitungsprozesse beteiligt.

➔ **Ohne die vertragliche Übernahme der Verpflichtung zur Erstellung eines Verfahrensverzeichnisses ist ein Vertrag zur Auftragsdatenverarbeitung nicht gültig!**

§ 32 Zusammenarbeit mit der Datenschutzaufsicht

Die Verpflichtung zur Zusammenarbeit mit der Aufsicht gilt auch für den Auftragsverarbeiter. Sie muss vertraglich eindeutig festgelegt werden.

§ 33 Absatz 2 Meldung an die Datenschutzaufsicht

Der Auftragnehmer hat den Verantwortlichen zu unterrichten, wenn ihm die Verletzung von Datenschutzvorschriften bekannt wird. Damit wird dem Verantwortlichen die Möglichkeit gegeben, die Aufsichtsbehörde nach Absatz 1 zu unterrichten und geeignete Abhilfemaßnahmen durchzu-führen. Dabei ist auch die dem Verantwortlichen für die Meldung gesetzte Frist von 72 Stunden zu berücksichtigen, mit der Folge, dass die Mitteilung des Auftragnehmers unverzüglich, also ohne schuldhaftes Zögern, zu erfolgen hat.

Diese Hinweise führen zu der anliegenden Formulierungshilfe.

Auf Grund dieses Vorschlages können individuelle Vereinbarungen zwischen den Parteien getroffen werden. Dabei sind alle hier erwähnten Punkte mit in die Vereinbarung einzubeziehen. Weitere Vereinbarungen können hinzukommen, wie beispielsweise die Wartung der Systeme oder die externe Datenarchivierung.

* * *

Formulierungshilfe
für die Erstellung von Verträgen
zur Verarbeitung personenbezogener Daten
bei vertragsärztlichen Leistungen durch beauftragte Unternehmen

_____

(Verantwortlicher Auftraggeber[3])

_____

(Auftragsverarbeiter[4])

1. Gegenstand des Auftrags, § 29 Abs. 3 lit. a) KDG

Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers die Abrechnung der von ihm erbrachten stationären und ambulanten vertragsärztlichen Leistungen.

Der Auftraggeber überlässt dem Auftragnehmer hierfür alle Daten und Unterlagen, die für die Erstellung einer ordnungsgemäßen und vollständigen Abrechnung der erbrachten Leistungen geeignet und erforderlich sind, in einem bearbeitungsfähigen Zustand. Der Auftraggeber wird alle Informationen, die nicht verarbeitungsfähig sind,

3 Die Vertragspartner sind richtig und vollständig auch nach ihrer Rechtsform, dem Träger und ihren Vertretungsverhältnissen (also nach den zeichungsberechtigten Personen) zu benennen. Zur Vereinfachung sollte hier festgelegt werden, dass das Krankenhaus im Vertragstext als „Auftraggeber“ und der Auftragsverarbeiter als „Auftragsnehmer“ bezeichnet wird.

4 siehe Fußnote 3

(etwa, weil sie nicht den ICD-10-GM-Code oder nicht den OPS-301-Schlüssel oder nicht die Zusatzkennzeichnung des Diagnoseschlüssels oder offensichtlich fehlerhafte oder unschlüssige Informationen enthalten) unbearbeitet an den Auftraggeber zur Korrektur zurücksenden. Der Auftragnehmer nimmt keine eigenmächtigen Korrekturen vor.

Die Abrechnung erfolgt unter der Arztnummer und der Betriebsstätten Nummer des Auftraggebers. Änderungen hieran, sind dem Auftragnehmer durch den Auftraggeber mitzuteilen.

Der Auftragnehmer darf die ihm überlassenen und von ihm ermittelten Daten ausschließlich für die ihm in diesem Vertrag übertragenen Zwecke nutzen. Er ist dabei an die Weisungen des Auftraggebers gebunden. Jede zweckwidrige Verwendung der Daten gilt als schwerwiegender Vertragsbruch. Strafrechtliche und andere gesetzliche Sanktionen bleiben unberührt.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einemMitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Zum Zeitpunkt des Vertragsabschlusses erfolgt die Datenverarbeitung in Deutschland und zwar in den Rechenzentren des Auftragnehmers in
<*ANSCHRIFT DATENVERARBEITUNG*>.

2. Dauer des Auftrags, § 29 Abs. 3 lit. b) KDG

Der Vertrag beginnt am <*DATUM VERTRAGSBEGINN*> und wird auf unbestimmte Zeit abgeschlossen.

Er kann von einem Vertragspartner aus wichtigem Grund fristlos, ohne Angabe von Gründen unter Einhaltung einer Frist von drei Monaten zum Quartalsende, oder im Einvernehmen der Vertragsparteien durch schriftliche Kündigung aufgelöst werden. Ein wichtiger Grund liegt insbesondere dann vor, wenn ein grob vertragswidriges Verhalten durch nachhaltigen Verstoß gegen datenschutzrechtliche Regelungen dieses Vertrages oder gegen gesetzliche

Vorschriften nach § 29 Abs. 4 und 5 KDG festgestellt wird, der Auftragnehmer nicht im Stande oder bereit ist, Weisungen des Auftraggebers zu befolgen oder dessen Kontrollrechte behindert.

3. Art und Zweck der Verarbeitung, § 29 Abs. 3 lit c) KDG

Die Verarbeitung dient der Geltendmachung und Einziehung, der dem Auftraggeber für die von ihm erbrachten medizinischen Leistungen zustehenden Vergütungen gegenüber selbstzahlenden oder privatversicherten Patienten. Diese sind gegenüber den behandelten Personen und bei Vorliegen einer schriftlichen Kostenübernahmebestätigung seitens der Privaten Krankenversicherung auch dieser gegenüber abzurechnen. Vorausleistungen des Patienten oder seiner Versicherung sind zu berücksichtigen.

Die Abrechnung wird vom Auftragnehmer nach den Bestimmungen der Gebührenordnungen[5] GOÄ, UVGOÄ, GOP, GebüH ordnungsgemäß und in nachvollziehbarer, plausibler Weise korrekt durchgeführt. Alle Vorgänge, insbesondere Rechnungsstellungen und der Erhalt von Teil- oder Gesamtzahlungen sind nach anerkannten buchhalterischen Regeln zu erfassen und dem Auftraggeber monatlich zur Verfügung zu stellen. Dabei werden dem Auftraggeber folgende Auswertungen zur Verfügung gestellt:

a) Sachstandsbericht über Rechnungsstellungen, Zahlungen und offene Posten.
b) Auswertungen bezüglich der einzelnen Fachabteilungen.
c) …..

4. Art der personenbezogenen Daten, Kategorien betroffener Personen, § 29 Abs. 3 lit d) bis e) KDG

Verarbeitet werden die personenbezogenen Daten von Patienten, deren Kosten nicht von gesetzlichen Krankenkassen getragen werden (Privatpatienten). Bei Minderjährigkeit des Patienten erfolgt zudem die Verarbeitung der Daten der Sorgeberechtigten und Versicherungsnehmer, in deren Vertag die Minderjährigen einbezogen sind.

Der Auftraggeber überlässt dem Auftragnehmer hierzu folgende Daten:

a) die Stammdaten des Patienten, vollständiger Name, Geburtsdatum, aktuelle Wohnanschrift;

5 Nicht anzuwendende Gebührenordnungen sind zu streichen

b) die Stammdaten des Versicherungsnehmers, vollständiger Name, aktuelle Wohnanschrift falls dieser von Ziffer a) abweicht;
c) die Zeit der Behandlung unter Angabe der Termine der Aufnahme und Entlassung;
d) die Beschreibung für die im Rahmen der Untersuchung, Beratung und Behandlung des Patienten erbrachten Leistungen einschließlich der erfolgten Diagnose;
e) die vom Auftraggeber eingesetzte Medikation des Patienten;
f) die im Rahmen der Behandlung und Rehabilitation zusätzlich eingesetzten Hilfsmittel;
g) besonders abrechenbare weitere Leistungen (Wahlleistungen).

5. Pflichten und Rechte des Auftraggebers, § 29 Abs. 3 lit. f) KDG

Die Zulässigkeit der Verarbeitung liegt nach § 6 Abs. 1 KDG allein im Verantwortungsbereich des Auftraggebers. Ebenso hat der Auftraggeber sämtliche Informationspflichten gegenüber den betroffenen Personen nach §§ 14 bis 25 KDG wahrzunehmen. Der Auftragnehmer wird aber den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen darin unterstützen, seiner Verantwortung insoweit nachkommen zu können.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in ei-nem, zwischen den Parteien vereinbarten elektronischen Format. Sind mündliche Weisungen nicht zu umgehen, so sind sie unverzüglich schriftlich oder in dem vereinbarten elektronischen Format zu bestätigen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind zwischen den Parteien abzustimmen und schriftlich oder elektronisch festzulegen.

Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig von der Einhaltung der beim Auftraggeber getroffenen Maßnahmen und die Einhaltung der Pflichten aus diesem Vertrag zu überzeugen. Der Auftragnehmer wird ihn dabei, soweit erforderlich unterstützen. Der Auftraggeber ist jedoch verpflichtet, alle ihm bekannt gewordenen geschäftlichen Angelegenheiten des Auftragnehmers und die von ihm getroffenen Datensicherheitsmaßnahmen vertraulich zu behandeln.

Nach § 29 Abs. 4 lit. h) KDG wird eine Prüfung alle <*ANGABE JAHRE, EMPFEHLUNG: „2“*> durch den Betriebsbeauftragten des Auftraggebers und weitere von ihm eingesetzten Hilfskräften durchgeführt. Sie erfolgt erstmalig am <*DATUM*>. Die Prüfung wird mindestens 14 Tage vorher angekündigt und der genaue Termin mit dem Auftragnehmer abgestimmt.

Zur Vorbereitung sind dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Verpflichtungen des Auftragnehmers, insbesondere eine aktuelle Beschreibung der von ihm nach § 26 KDG getroffenen technischen und organisatorischen Maßnahmen und das Verzeichnis der Verarbeitungstätigkeiten nach § 31 Abs. 2 KDG zu übermitteln. Stellt der Auftraggeber bei der Prüfung Fehler oder Unregelmäßigkeiten fest, ist der Auftragnehmer unverzüglich hierüber zu informieren. Das Ergebnis der Prüfung ist vom Auftraggeber in einem schriftlichen Bericht festzuhalten.

Hierbei erklären die Vertragspartner übereinstimmend, dass eine Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) nicht stattfindet.

6. Weisungsberechtigte Personen und Weisungsempfänger

Weisungsberechtigte Personen des Auftraggebers sind:

<VORNAME, NAME, ORGANISATIONSEINHEIT, TELEFON, PERSONIFIZIERTE E-MAIL-ADRESSE>

und als Vertreter in allen Abwesenheitsfällen

<VORNAME, NAME, ORGANISATIONSEINHEIT, TELEFON, PERSONIFIZIERTE E-MAIL-ADRESSE>

Weisungsempfänger beim Auftragnehmer sind:

<VORNAME, NAME, ORGANISATIONSEINHEIT, TELEFON, PERSONIFIZIERTE E-MAIL-ADRESSE>

Und falls dieser nicht erreichbar ist sein Vertreter:

<VORNAME, NAME, ORGANISATIONSEINHEIT, TELEFON, PERSONIFIZIERTE E-MAIL-ADRESSE>

7. Pflichten des Auftragnehmers, § 29 Absätze 4, 5, 11 und § 30 KDG

a) Verarbeitung nach Weisung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der hier getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Kirchliche Recht, das Recht der Europäischen Union oder das Recht ihrer Mitgliedsstaaten, 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 öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

b) Zweckbindung der Daten

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

c) Trennung der Datenbestände

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt wer-den, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

<AUFZÄHLUNG DER ÜBERPRÜFUNGEN>

Das Ergebnis der Kontrollen ist zu dokumentieren.

d) Mitwirkung des Auftragnehmers

Sowohl bei der Erfüllung der Rechte der betroffenen Personen nach §§ 15 bis 25 KDG durch den Auftraggeber, wie auch an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten und bei erforderlichen Datenschutz-Folgenabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (§ 29 Abs. 4 lit. e) und f) KDG). Er hat die dazu erforderlichen

Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:
<*ANGABE STELLE AUFTRAGGEBER*>

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (§ 29 Abs. 4 lit. h) Satz 2 KDG). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

e) Berichtigung, Löschung und Auskunft über die verarbeiteten Daten
Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.
Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

f) Rechtliche Bestimmungen
Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften des KDG bekannt sind.

Anmerkung: Zur Wahrung der Berufsgeheimnisse nach § 203 StGB sollte ebenfalls eine Regelung vereinbart werden, die sowohl den Auftraggeber (§ 203 Abs. 1 Nr. 1, 2 StGB) wie auch ihn als Auftragnehmer (§ 203 Abs. 1 Nr. 7 StGB) verpflichtet.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (§ 29 Abs. 4 lit. b) KDG). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Der Auftragnehmer unterliegt der Datenschutzaufsicht des Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes <*NAME BUNDESLAND*>.

Der Auftragnehmer hat eine(n) Beauftragte(n) für den Datenschutz bestellt. Ihre/Seine Tätigkeit ist der Aufsichtsbehörde nach Art. 37 Abs. 7 DSGVO mitgeteilt worden. Zurzeit wird diese Aufgabe wahrgenommen von Herrn/Frau

<VORNAME, NAME, ORGANISATIONSEINHEIT, TELEFON>

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

g) Mitteilungspflichten des Auftragnehmers
Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, insbesondere Verstöße des Auftragnehmers selbst oder der bei ihm beschäftigten Personen mit. Das gilt besonders bei einem Verdacht auf Verletzung datenschutzrechtlicher Bestimmungen oder dem Auftauchen von Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten. Die Mitteilung umfasst mindestens die in § 33 Abs. 3 KDG festgelegten Informationen. Hiermit wird der Auftraggeber in die Lage versetzt, die Notwendigkeit einer Meldung an die Aufsichtsbehörde nach § 33 Abs. 1 KDG zu prüfen und gegebenenfalls vorzunehmen.

Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei der Einhaltung seiner Pflichten nach §§ 33, 34 KDG angemessen zu unterstützen (§ 29 Abs. 4 lit. f) KDG).

Meldungen an die Aufsichtsbehörde nach § 33 Abs. 1 KDG und die Benachrichtigung von betroffenen Personen nach § 34 KDG für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 6 dieses Vertrages durchführen.

8. Unterauftragsverhältnisse, § 29 Abs. 2 KDG

Zum Zeitpunkt des Abschlusses dieses Vertrages vereinbaren die Parteien,

<ALTERNATIVE 1:>
dass keine Verarbeitung der personenbezogenen Daten nach Ziffer 4 dieser Vereinbarung von einem weiteren Auftragsverarbeiter im Rahmen eines Unterauftragsverhältnisses erbracht werden. Der Auftragnehmer ist sich dabei bewusst, dass er nach § 29 Abs. 2 KDG auch künftig, nur nach vorhergehender schriftlicher Genehmigung des Auftraggebers einen wei-teren Auftragsverarbeiter beauftragen kann.

<ALTERNATIVE 2:>
dass folgende Arbeiten
<AUFZÄHLUNG DER ARBEITEN>
in einem Unterauftragsverhältnis und auf Grund des Vertrages vom <VERTRAGSDATUM> von der Firma <FIRMENNAME> erbracht werden. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter ist dem Auftraggeber abschriftlich zur Verfügung gestellt worden. Er hat sich auf Grund dessen davon überzeugt, dass der Unterauftragsvertrag die gleichen rechtlichen Verpflichtungen enthält, wie sie in diesem Vertrag zwischen den Parteien vereinbart worden sind. Ihm wurde zudem ein Verzeichnis der von Unterauftragsnehmer zu erbringenden Verarbeitungstätigkeiten und eine verbindliche Beschreibung der technisch-organisatorischen Maßnahmen nach § 26 KDG vorgelegt.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:
<AUFZÄHLUNG PRÜFAKTIVITÄTEN>

Das Ergebnis der Überprüfungen ist schriftlich zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.
Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

09. Technische und organisatorische Maßnahmen nach §§ 26, 29 Abs. 4 lit. c) KDG

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von § 27 Abs. 1 KDG, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

<Alternative 1>:
Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

<ANGABE ZUR METHODIK DER RISIKOBEWERTUNG>

Das im Anhang <BEZEICHNUNG ANHANG> beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.
Das im Anhang <BEZEICHNUNG ANHANG> beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

oder

<ALTERNATIVE 2:>
Der Auftragnehmer arbeitet nach einem Verfahren, das von einer nach Art. 43 DSGVO akkreditierten Zertifizierungsstelle nach Art. 42 DSGVO zertifiziert worden ist. Dieses wird als Nachweis für hinreichende Garantien über ausreichende technisch-organisatorische Maßnahmen zum Schutz der Rechte der Betroffenen angesehen (§ 29 Abs. 6 KDG).

Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragnehmers wurden am <DATUM> durch die folgende unabhängige externe Stellen auditiert/zertifiziert gemäß den Regelungen nach Art. 42:
<NAME DER EXTERNEN STELLE>

Die vollständigen Prüfunterlagen und Auditberichte wurden vom Auftraggeber eingesehen und werden ihm auf Wunsch jederzeit wieder zur Einsichtnahme ausgehändigt.

10. Verpflichtungen des Auftragnehmers nach Erbringung der Verarbeitungsleistungen, Art. 29 Abs. 4 lit. g) KDG

<ALTERNATIVE 1:>
Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

oder

<ALTERNATIVE 2:>
Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:
<ANGABE ZUM LÖSCHVERFAHREN>

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

11. Vergütung der Tätigkeit

Die seitens des Auftraggebers zu zahlenden Entgelte für die Leistungen des Auftragnehmers werden in einem gesonderten Vertrag vereinbart.

12. Haftung

Die Haftung wegen eines Verstoßes nach diesem Gesetz gegenüber der betroffenen Person richtet sich nach § 50 KDG.

13. Vertragsstrafe

Bei Verstoß des Auftragnehmers gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von *<ANGABE BETRAG>* Euro vereinbart.

14. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

15. Gerichtsstand, salvatorische Klausel und Rechtsnachfolge

Für Nebenabreden ist grundsätzlich die Schriftform erforderlich.
Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Falls eine Bestimmung dieses Vertrages unwirksam sein oder werden sollte, wird sie durch eine zulässige Vereinbarung ersetzt, die dem Ziel der jetzigen Vereinbarung am nächsten kommt.

Es gilt deutsches Recht. Gerichtsstand und Erfüllungsort ist, soweit nicht anders vereinbart, <ANGABE DES GERICHTSSTANDS>.

Die beiderseitigen Rechte und Pflichten dieses Vertrages gehen auf die jeweiligen Rechtsnachfolger der Vertragsparteien über.

Anlage

Erwägungsgrund 81 DS-GVO

Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden. Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Erwägungsgrund 168 DS-GVO

Für den Erlass von Durchführungsrechtsakten bezüglich Standardvertragsklauseln für Verträge zwischen Verantwortlichen und Auftragsverarbeitern sowie zwischen Auftragsverarbeitern; Verhaltensregeln; technische Standards und Verfahren für die Zertifizierung; Anforderungen an die Angemessenheit des Datenschutzniveaus in einem Drittland, einem Gebiet oder bestimmten Sektor dieses Drittlands oder in einer internationalen Organisation; Standardschutzklauseln; Formate und Verfahren für den Informationsaustausch zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden im Hinblick auf verbindliche interne Datenschutzvorschriften; Amtshilfe; sowie Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Ausschuss sollte das Prüfverfahren angewandt werden.

Diese Arbeitshilfe 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