Formulierungshilfe

Vertrag zur Fernwartung

gemäß dem Gesetz über den kirchlichen Datenschutz (KDG)

Stand 04/2018

Konferenz der Diözesandatenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Formulierungshilfe

Vertrag zur Fernwartung zwischen kirchlichem Auftraggeber und nichtkirchlichem Auftragnehmer

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
Vertrag zur Fernwartung zwischen kirchlichem Auftraggeber und nichtkirchlichem Auftragnehmer

Vereinbarung

zwischen <*Name Auftragnehmer*>, nachstehend Auftragnehmer genannt
und <*Name Auftraggeber*>, nachstehend Auftraggeber genannt

§ 1 Gegenstand der Vereinbarung

Der Auftraggeber betreibt in <*Anschrift Auftraggeber*> EDV-Systeme mit folgenden Komponenten:
<*hier sind die vorhandenen Systeme so genau als möglich zu beschreiben*>

Der Auftragnehmer führt an diesen Systemen Fernwartungsarbeiten im Auftrag des Auftraggebers durch.
Diese Vereinbarung umfasst folgende, vom Auftragnehmer durchzuführende Fernwartungsarbeiten:
<*Hier sind folgende Punkte im Einzelnen aufzuführen:*

- *Systeme, auf die per Fernwartung zugegriffen werden soll*
- *Softwareprodukte, die der Fernwartung unterliegen*
- *Umfang, Art und Zweck der Fernwartung (z. B. Fehlerbehebung, Störfalldefinition, Updates, Upgrades, Patches)*
- *Softwareprodukte, die bei der Fernwartung eingesetzt werden sollen*
- *Umfang der Zugriffe (Dateien, Verzeichnisse, schreibender oder lesender Zugriff)*
- *Art der personenbezogenen Daten, die vom Zugriff betroffen sein können*
- *Vom Zugriff ausgenommene Systeme und Softwareprodukte*
- *Kreis der Betroffenen*>

§ 2 Schriftformklausel

(1) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen im Rahmen der Fernwartung können nur schriftlich vereinbart werden.(2) Nachrichten der Vertragsparteien, die elektronisch übertragen werden, können nur akzeptiert werden, wenn sie mit einer digitalen Signatur versehen sind.

§ 3 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Fernwartung sowie für die Wahrung der Rechte der Betroffenen bleibt der Auftraggeber verantwortlich. Personenbezogene Daten, die zur Erfüllung dieses Vertrags weitergegeben werden, dürfen nur verwendet werden, soweit dies für die Zwecke der Fernwartung zwingend erforderlich ist und der Auftraggeber hiervon vorab in Kenntnis gesetzt wurde.

(2) *<fakultativ: Der Auftraggeber richtet auf folgenden Datenbanken mindestens je 20 Datensätze mit nicht wirklich existierenden Daten ein: <Aufzählung der Datensätze> und teilt dies dem Auftragnehmer mit. Ist dies der Fall, dürfen Versuche mit Wartungsarbeiten durch den Auftragnehmer nur mit diesen Daten ausgeführt werden.>*

(3) Der Auftraggeber ist berechtigt, Anweisungen über Art, Umfang und Ablauf der Fernwartung zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Weisungsberechtigte Personen des Auftraggebers sind:

- *<Aufzählung mit Name/Bezeichnung>*

Weisungsempfänger beim Auftragnehmer sind
als Verantwortlicher: *<Name/Bezeichnung>*
als betrieblicher Datenschutzbeauftragter: *<Name/Bezeichnung>*

< fakultativ: Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die Voraussetzungen für eine Bestellung nicht vorliegen.>

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners wird dem Vertragspartner binnen zwei Werktagen schriftlich der Nachfolger beziehungsweise der Vertreter mitgeteilt.

(4) Der Auftraggeber überwacht die Fernwartung. Alle Zugriffe, die im Rahmen der Fernwartung in Systemen des Auftraggebers erfolgen, werden protokolliert. Die Protokollierung muss revisionssicher sein und darf vom Auftragnehmer nicht abgeschaltet

werden.

(5) Der Auftraggeber informiert den Auftragnehmer sofort, wenn Fehler oder Unregelmäßigkeiten bei der Fernwartung festgestellt werden, insbesondere die, die einen Zugriff durch Unbefugte ermöglichen können.

(6) Der Auftraggeber unterbricht einen unbefugten Zugriff und überprüft, von wem der unbefugte Zugriff ausging und ob die technischen und organisatorischen Maßnahmen ausreichen, um zukünftig einen unbefugten Zugriff zu verhindern; gegebenenfalls weist er weitere technische und organisatorische Maßnahmen an.

(7) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers geheim zu halten und in keinem Fall Dritten zu offenbaren.

<Bei Fernwartung im Anwendungsbereich des § 80 SGB X:

(8) Der Auftraggeber zeigt die Auftragserteilung gemäß § 80 Absatz 7 SGB X dem Ordinariat <Name der Erz-/Diözese> schriftlich an.>

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer handelt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er darf personenbezogene Daten nur entsprechend § 3 Absatz 1 Satz 2 dieses Vertrages verwenden. Es werden keine Kopien oder Duplikate ohne Wissen des Auftraggebers erstellt. Soweit möglich, erfolgt die Fernwartung am Bildschirm ohne gleichzeitige Speicherung.

(2) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zu offenbaren.

(3) Der Auftragnehmer erkennt insbesondere an, dass er für die Auftragsdatenverarbeitung das Kirchliche Datenschutzgesetz einzuhalten hat und unterwirft sich insofern der Kontrolle des zuständigen Diözesandatenschutzbeauftragten. Ein Abdruck des Kirchlichen Datenschutzgesetzes wurde ihm ausgehändigt.

(3) Die Anforderungen an die Verarbeitung personenbezogener Daten im Auftrag gelten nach § 29 Absatz 12 KDG auch für die Fernwartung.

(4) Der Auftragnehmer erkennt an, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz, der technischen und organisatorischen Maßnahmen und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige

Kontrollen vor Ort. Der Auftragnehmer sagt seine Mitwirkung bei diesen Kontrollen zu.

(5) Die Verarbeitung und Nutzung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder der Schweiz statt.

(6) Entscheidungen zur Organisation und Durchführung der Fernwartung, insbesondere sicherheitsrelevante Entscheidungen, sind mit dem Auftraggeber abzustimmen und schriftlich zu fixieren.

(7) Der Auftragnehmer informiert den Auftraggeber unverzüglich, sobald eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Die Durchführung der betroffenen Weisung kann durch den Auftragnehmer solange ausgesetzt werden, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(8) Eine Beauftragung von Unterauftragnehmern wird ausgeschlossen.
<fakultativ: Die Beauftragung von Unterauftragnehmern ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Es gelten die Vereinbarungen aus Anlage <Name der Anlage> oder <Name der Anlage>.

(9) Der Auftragnehmer hat mindestens folgende Kontrollmaßnahmen durchzuführen:
- *<Aufzählung der Kontrollmaßnahmen>*

(10) Der Auftragnehmer hat an der Erstellung der Verzeichnisse über Verarbeitungsvorgängen mitzuwirken. Die erforderlichen Angaben hat er dem Auftraggeber zuzuleiten.

(11) Vor Beginn der Fernwartung teilt der Auftragnehmer dem Auftraggeber mit (schriftlich oder in der Form des § 2 Absatz), welche Mitarbeiter er dafür einsetzen wird und wie diese Mitarbeiter sich identifizieren werden. Die Mitarbeiter des Auftragnehmers verwenden hinreichend sichere, vom Auftraggeber freigegebene Identifizierungsverfahren.

(12) Fernwartungen werden ausschließlich von der Wartungszentrale aus vorgenommen, deren Sicherheitsmaßnahmen in § 7 Absatz 1 vereinbart worden sind. Ein Fernwartungszugriff ist nur mit Hilfe der vom Auftraggeber freigegebenen Software zulässig.

(13) Der Auftragnehmer kündigt den Beginn der Fernwartung telefonisch an, um dem Auftraggeber, ggf. durch Beauftragte, die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen. Ein Fernwartungszugriff ohne Wissen des Auftraggebers, vertreten durch den Nutzer des Systems, ist nicht zulässig. Dies soll, sofern möglich, durch technische Maßnahmen sichergestellt sein.

(14) Der Auftragnehmer erkennt an, dass der Auftraggeber jederzeit berechtigt ist, die Fern-

wartung zu unterbrechen, insbesondere wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird. Die Unterbrechung kann insbesondere erfolgen, wenn eine Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten festgestellt wird.

(15) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen verschlüsselt in einem angemessenen Verhältnis zu dem Schutzzweck und dem Stand der Technik gemäß erfolgen.

(16) Datenträger, die für den Auftraggeber genutzt werden oder von ihm stammen, werden besonders gekennzeichnet. Eingang und Ausgang werden dokumentiert.

(17) Wurden personenbezogene Daten des Auftraggebers während der Fernwartung oder der dabei erforderlichen Tests kopiert, so sind diese nach Abschluss der konkreten Fernwartungsmaßnahme unverzüglich in Abstimmung mit dem Auftraggeber zu löschen oder dem Auftraggeber zu übergeben. In den Besitz des Auftragnehmers gelangte Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, werden ebenfalls ausgehändigt. Ausgenommen sind Daten, die zur Dokumentationskontrolle und für Revisionsmaßnahmen der Fernwartung benötigt werden.

(18) Nicht mehr benötigte Unterlagen und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

§ 5 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, das Datengeheimnis gemäß § 5 KDG zu wahren.

(2) Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten wie sie dem Auftraggeber obliegen.

(3) Der Auftragnehmer verpflichtet sich, die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut zu machen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften; im Fall der Erteilung von Unteraufträgen gilt das auch gegenüber den in Anlage zu diesem Vertrag genannten Unterauftragnehmern.

(4) Der Auftragnehmer darf keine Auskünfte an Dritte erteilen, Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen (§ 3 Absatz 2) erteilen.

§ 6 Kontrollrechte

Der Auftragnehmer verpflichtet sich, dem Diözesandatenschutzbeauftragten und den ihm eingesetzten Mitarbeitern Zugang zu seinen Arbeitsräumen zu gewähren und unterwirft sich deren Kontrolle .

§ 7 Technische und organisatorische Maßnahmen

(1) Für die auftragsgemäße Bearbeitung personenbezogener Daten nutzt der Auftragnehmer folgende technischen Einrichtungen:
- *<Aufzählung/Benennung der verwendeten Hardware und Software>*

(2) Das als Anlage beigefügte Datenschutzkonzept des Auftragnehmers wird als verbindlich festgelegt
<fakultativ: Die folgenden beziehungsweise in Anlage <Name der Anlage> beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.>

(3) Um die Übertragung der Daten abzusichern und unbefugte Zugriffe auf die Systeme des Auftraggebers im Rahmen der Fernwartung zu verhindern, legt der Auftraggeber folgende technische und organisatorische Maßnahmen für beide Seiten bindend fest:
1. Zutrittskontrolle …
2. Zugangskontrolle …
3. Zugriffskontrolle …
4. Weitergabekontrolle …
5. Eingabekontrolle …
6. Auftragskontrolle …
7. Verfügbarkeitskontrolle …
8. Zwecktrennung …

(4) Der Auftragnehmer gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen und beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung.

(5) Die technischen und organisatorischen Maßnahmen können während des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Für wesentliche Änderungen ist eine schriftliche Vereinbarung notwendig.

(6) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, seine Verstöße, diejenigen des Unterauftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen

sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

§ 8 Mitgeltende Regelungen

Neben den festgelegten technischen und organisatorischen Maßnahmen sind folgende Regelungen ebenfalls für beide Seiten verbindlich:
<Beschreibung der Regelungen>

§ 9 Vertragsdauer

(1) Der Vertrag
<beginnt am <Beginndatum> und endet am <Endedatum/mit Auftragserledigung/ wird auf unbestimmte Zeit geschlossen.>
Er ist mit einer Frist von <Fristdauer> Monaten zum <Datum> kündbar.>

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers oder des Unterauftragnehmers gegen die Bestimmungen des Kirchlichen Datenschutzgesetzes oder dieses Vertrages vorliegt, der Auftragnehmer oder der Unterauftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der Landesbeauftragten für Datenschutz und Informationsfreiheit vertragswidrig verweigert.

<fakultativ: § 10 Vergütung

sofern vereinbart>

§ 11 Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter beziehungsweise die von ihm ggfs. eingeschalteten Unterbeauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem KDG, der EU-DS-GVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Dem Auftragnehmer bleibt

der Rückgriff beim Auftragnehmer vorbehalten, soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist.

<fakultativ: § 12 Vertragsstrafev

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von <Höhe Vertragsstrafe>€ vereinbart.>

<fakultativ: § 13 Nichterfüllung der Leistung

sofern vereinbart>

§ 14 Sonstiges

(1) Der Auftragnehmer gibt dem Auftraggeber zur Sicherung die mobilen Datenträger zurück, auf denen sich Dateien befinden, welche personenbezogene Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen.
(2) Sollten Daten des Auftraggebers beim Auftragnehmer oder beim Unterauftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Begebenheiten gefährdet werden, so hat der Auftragnehmer oder der Unterauftragnehmer den Auftraggeber unverzüglich zu verständigen.
(3) Für Nebenabreden ist die Schriftform erforderlich.
(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 Bürgerliches Gesetzbuch wird hinsichtlich der verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen.

§ 15 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

<fakultativ: Anlage zur Vereinbarung

Ausführungen zum Verhältnis zwischen Auftragnehmer und Unterauftragnehmer

(1) Die Beauftragung von Unterauftragnehmern ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer Namen und Anschrift des Unterauftragnehmers mitteilt.

(2) Außerdem muss der Auftragnehmer versichern, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat.

(3) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Unterauftragnehmer gelten.

(4) Der Auftraggeber ist berechtigt, Kontrollen vor Ort beim Unterauftragnehmer durchzuführen oder durch Dritte durchführen zu lassen. Der Auftragnehmer hat die Einhaltung der Pflichten regelmäßig beim Unterauftragnehmer zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren.

(5) Der Unterauftragnehmer erkennt insbesondere an, dass er für die Auftragsdatenverarbeitung das Kirchliche Datenschutzgesetz einzuhalten hat und unterwirft sich insofern der Kontrolle des zuständigen Diözesandatenschutzbeauftragten. Einen Abdruck erhält er vom Auftragnehmer.

(6) Der Unterauftragnehmer verpflichtet sich insbesondere, dem zuständigen Diözesandatenschutzbeauftragten und den ihm eingesetzten Bediensteten Zugang zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle insoweit nach Maßgabe des Kirchlichen Datenschutzgesetzes. Er benachrichtigt sowohl den Auftragnehmer als auch den Auftraggeber, bevor eine angekündigte Kontrolle stattfindet.

(7) Die Weiterleitung von personenbezogenen Daten ist erst zulässig, wenn der Unterauftragnehmer die Verpflichtungen nach § 29 Kirchliches Datenschutzgesetz erfüllt hat. In dem Vertrag mit dem Unterauftragnehmer sind die Aufgaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern.

(8) Der Auftragnehmer hat vertraglich sicherzustellen, dass die Verarbeitung und Nutzung der personenbezogenen Daten durch den Unterauftragnehmer ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen

Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder der Schweiz stattfindet. Jede Verlagerung in einen Drittstaat bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen des § 40 Kirchliches Datenschutzgesetz erfüllt sind.

(9) Die Unterauftragnehmer, die mit der Verarbeitung von personenbezogenen Daten in dem in der Vereinbarung genannten Umfang beschäftigt sind, sind mit Namen, Anschrift und Auftragsinhalt dem Auftraggeber zu benennen. Der Auftraggeber muss sich schriftlich mit deren Beauftragung einverstanden erklären.>

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