



## Der Diözesandatenschutzbeauftragte

der Erzbistümer Berlin und Hamburg,  
der Bistümer Hildesheim, Magdeburg, Osnabrück und  
des Bischöflich Münsterschen Offizialats in Vechta i.O.

### **Mustervertrag zur Auftragsdatenverarbeitung nach § 8 KDO<sup>1</sup>**

(Stand: 22. Februar 2011)

#### **Vorbemerkung:**

Der nachfolgende Mustervertrag soll es kirchlichen Stellen erleichtern, mit Auftragnehmern ausreichende vertragliche Regelungen unter Beachtung von § 8 der Anordnung über den kirchlichen Datenschutz - KDO - zu vereinbaren. Dabei ist der Inhalt des Vertrages jeweils aufgabenspezifisch anzupassen. Das darf allerdings nicht dazu führen, dass das hier vorgegebene Schutzniveau unterschritten wird.

Die genannte Vorschrift stellt hohe Anforderungen im Hinblick auf den Schutz des Persönlichkeitsrechts der Betroffenen, mit deren Daten sorgfältig umzugehen ist. Für den schriftlichen Auftrag sind gesetzlich eine Reihe von Mindestanforderungen vorgegeben. So sind die Datenerhebung, -verarbeitung und -nutzung sowie die technisch-organisatorischen Maßnahmen zum Schutz der Daten vertraglich festzulegen. Dies kann nur durch eine zweiseitige, schriftliche Vereinbarung geschehen. Einseitige, sog. "Datenschutzerklärungen" des Auftragnehmers reichen hier auf keinen Fall aus! Daher bitte die Finger lassen von Auftragnehmern die nicht bereit sind, einen schriftlichen Vertrag nach dem hier veröffentlichten Muster abzuschließen. Seriöse Vertragspartner werden immer auch Verständnis dafür haben, dass der Auftraggeber sich rechtlich absichern will und muss. Folgt man der hier vorgeschlagenen Regelung, sind die Voraussetzungen nach § 8 KDO vollständig erfüllt.

Die hier vorgestellte Mustervereinbarung folgt im wesentlichen den Musterverträgen, wie sie von den staatlichen Aufsichtsinstanzen für die Auftragsdatenverarbeitung zwischen öffentlichen Stellen und öffentlichen oder nicht-öffentlichen Auftragnehmern entwickelt worden sind (veröffentlicht auf den Webseiten der LfD's von Bayern, Hessen, Saarland und Sachsen). Sie wurde an einigen Stellen geändert und den kirchlichen Rechtsverhältnissen angepasst.

Hannover, den 22. Februar 2011

---

<sup>1</sup> Eine Auftragsdatenverarbeitung ist nur in den Fällen zulässig, in denen das Gesetz nichts anderes bestimmt (z.B. § 203 StGB). In einigen Fällen sind besondere Anforderungen zu erfüllen (z.B. §§ 80 SGB X, 120 VI SGB V)

# Vereinbarung

zwischen dem/der

.....  
(nachstehend Auftragnehmer genannt)

und dem/der

.....  
(nachstehend Auftraggeber genannt)

## 1. Auftragnehmer<sup>2</sup>

Der Auftragnehmer ist ein gewerbliches (kirchliches) Unternehmen mit langjähriger Erfahrung auf dem Gebiet der Verarbeitung von .....daten. Er betreibt hierzu zwei Rechenzentren in ..... und ..... Der Firmensitz befindet sich in ....., so dass der Auftragnehmer der Aufsicht des Landesbeauftragten für den Datenschutz (des Diözesandatenschutzbeauftragten des Bistums) in ..... untersteht.

Der Auftragnehmer wendet die Vorschriften des Bundesdatenschutzgesetzes (der Anordnung über den kirchlichen Datenschutz) an. Er hat einen betrieblichen Datenschutzbeauftragten bestellt und seine Mitarbeiter schriftlich auf das Datengeheimnis verpflichtet. Sie werden regelmäßig geschult. Für die Rechenzentren besteht ein umfassendes Sicherheitskonzept, das dem Auftragnehmer bekannt ist. (Anlage 1). Änderungen dieses Konzepts sind dem Auftraggeber unverzüglich mitzuteilen.

## 2. Gegenstand der Vereinbarung

Der Auftragnehmer übernimmt die Verarbeitung der .....daten des Auftraggebers. Der Auftrag umfasst im Einzelnen folgende Arbeiten:

.....  
(Beschreibung der Aufgaben)

Die Beauftragung erfolgt in der gemeinsamen Überzeugung, dass der Auftragnehmer auf Grund seiner Leistungsfähigkeit und Spezialisierung die ihm übertragenen Arbeiten kostengünstiger und störungsfreier erledigen kann, als es dem Auftraggeber bisher möglich war.<sup>3</sup>

## 3. Rechte und Pflichten des Auftraggebers

Die Parteien stimmen darin überein, dass

<sup>2</sup> Nach § 8 Abs. 1 KDO ist der Auftragnehmer sorgfältig auszuwählen. Die Gründe, die zu seiner Beauftragung geführt haben, sollten am Anfang des Dokuments festgehalten werden. Dabei sollte auch festgestellt werden, dass der Auftragnehmer gerade für die hier in Rede stehende Verarbeitung personenbezogener Daten geeignet ist. Hierzu werden die wichtigsten technisch-organisatorischen Maßnahmen angesprochen. In der Vereinbarung liegt zugleich die Zusicherung einer genügenden Leistungsfähigkeit für die übernommene Aufgabe.

<sup>3</sup> In den Fällen von § 80 Abs. 5 SGB X ist der Zusatz zwingend erforderlich, sonst fakultativ.

- die Verantwortung für die ordnungsgemäße Durchführung der Datenverarbeitung sowie der Einhaltung der gesetzlichen Bestimmungen nach § 8 KDO beim Auftraggeber verbleibt. Die Rechte der Betroffenen nach § 5 KDO sind ihm gegenüber geltend zu machen.
- der Auftraggeber das Recht hat, sich vor Ort persönlich von der Einhaltung der beim Auftragnehmer getroffenen technisch-organisatorischen Maßnahmen zum Schutz der Daten zu überzeugen. Der Auftragnehmer ist insoweit verpflichtet, den Auftraggeber aktiv bei der Wahrnehmung dieses Rechts zu unterstützen, ihm insbesondere das Betreten der Geschäftsräume innerhalb der üblichen Geschäftszeiten sowie den Einblick in Unterlagen, die für die Sicherheit der Datenverarbeitung von Bedeutung sind, zu ermöglichen.
- der Auftraggeber das Recht hat, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Weisungsberechtigte Personen des Auftraggebers sind:

.....  
Weisungsempfänger beim Auftragnehmer sind:

.....  
Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

- Der Auftraggeber ist verpflichtet, den Auftragnehmer unverzüglich zu informieren, wenn Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse festgestellt werden.
- Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.
- Der Auftraggeber überlässt dem Auftragnehmer alle Daten und Unterlagen, die für die ordnungsgemäße und vollständige Durchführung der Arbeiten erforderlich sind in einem bearbeitungsfähigen Zustand. Fehlerhafte Daten oder Unterlagen werden zur Korrektur an den Auftraggeber zurückgegeben.
- Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

#### **4 Pflichten des Auftragnehmers**

Die Parteien stimmen weiterhin darin überein, dass

- Der Auftragnehmer personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers verarbeiten wird. Jede zweckwidrige Verwendung der Daten stellt einen schwerwiegenden Vertragsbruch dar. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.
- Der Auftragnehmer sichert im Bereich der auftragungsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen scharf getrennt werden.
- Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz 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.
- Der Auftragnehmer stellt dem Auftraggeber alle für die Verfahrensmeldung nach § 3a

Abs. 1, 2 KDO erforderlichen Angaben, insbesondere die über die zugriffsberechtigten Personen kontinuierlich zur Verfügung. Er fertigt für den Auftraggeber das Verzeichnis nach § 3a Abs. 4 KDO.

- Die Verarbeitung von Daten in Privatwohnungen ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den Auftraggeber vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.
- Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.
- Dem Auftragnehmer überlassene Datenträger sowie alle davon gefertigten Kopien, Sicherungen oder Reproduktionen bleiben das Eigentum des Auftraggebers. Sie sind besonders zu kennzeichnen und getrennt von anderen Datenträgern aufzubewahren. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer, unabhängig von eventuell offenen finanziellen oder sonstigen Forderungen, sämtliche in seinen Besitz gelangten Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber kostenfrei auszuhändigen. Vom Zeitpunkt der Kündigung an sind keine unbeauftragten Löschungen mehr vorzunehmen.
- Sollte das Eigentum 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 verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.<sup>4</sup>
- Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

## 5. Beauftragung von Subunternehmern

Die Beauftragung von Subunternehmen darf nur mit schriftlicher Zustimmung des Auftraggebers erfolgen. Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Der Auftragnehmer ist auch für die Handlungen, des von ihm beauftragten Subunternehmers haftbar.<sup>5</sup>

Die Weiterleitung der Daten des Auftraggebers ist erst zulässig, wenn die zuvor genannten Voraussetzungen erfüllt sind.

Die Einschaltung eines Subunternehmers darf nicht dazu führen, dass die Daten im Ausland, insbesondere in einem Land durchgeführt wird, dass keine ausreichenden Datenschutzbestimmungen erlassen und keine Kontrollbehörden zur Überwachung von Datenschutzbestimmungen eingerichtet hat (unsichere Drittländer).<sup>6</sup>

---

<sup>4</sup>Diese Klausel muss im Hinblick auf § 11 Nr. 2 AGB gesondert vereinbart werden.

<sup>5</sup> Auf diese Regelung sollte nicht verzichtet werden, da für den Auftraggeber oft schwer nachweisbar ist, wer die jeweilige Vertragsverletzung begangen hat.

<sup>6</sup> Hiermit soll verhindert werden, dass inländische Unternehmen Arbeiten in datenschutzrechtlich unsicheren Billiglohnländer durchführen.

## **6 Datengeheimnis**

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 4 KDO zu wahren. Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.<sup>7</sup>

Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften, einschließlich der Anordnung über den kirchlichen Datenschutz und der weiterhin geltenden bereichsspezifischen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut sind. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

Auskünfte an Betroffene oder Dritte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

## **7. Datensicherungsmaßnahmen**

Das von den Parteien vereinbarte Verfahren und die vom Auftragnehmer zum Schutz der dabei zu verarbeitenden Daten getroffenen technisch-organisatorischen Maßnahmen (§ 6 KDO) sind in einer Anlage zu diesem Vertrag ausführlich festgehalten (Anlage 2). Sie sind Bestandteil dieser Vereinbarung.

Das der Anlage 2 zugrunde liegende Datenschutzkonzept ist vom Auftragnehmer, dem jeweiligen Stand der Technik entsprechend, anzupassen und weiterzuentwickeln. Wesentliche Veränderungen sind mit dem Auftraggeber abzusprechen und in einer aktualisierten Fassung der Anlage 2 festzuhalten.

Stellt der Auftraggeber fest, dass die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen seinen Anforderungen nicht genügen, benachrichtigt er den Auftraggeber hierüber unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn eine vom ihm erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Auftraggeber geändert oder ausdrücklich bestätigt wird.

## **8. Vertragsdauer**

Der Vertrag beginnt am ..... und endet am .....

(Der Vertrag beginnt am ..... und endet mit der Erledigung des Auftrags.)

(Der Vertrag wird auf unbestimmte Zeit geschlossen.)

---

<sup>7</sup> Der Zusatz ist vor allem bei Tätigkeiten, die einer beruflichen Schweigepflicht unterliegen, zu beachten. Für privatärztliche Verrechnungsstellen ist anerkannt, dass sie als Gehilfen des Arztes anzusehen sind und § 203 StGB somit auch auf sie anwendbar ist.

Er ist mit einer Frist von ..... Wochen zum Quartalsende kündbar.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen der KDO oder dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer dem Auftraggeber den Zutritt zu seinen Räumen in vertragswidriger Weise verweigert.

## **9. Vergütung**

....

## **10. Haftung**

Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der KDO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

## **11 Vertragsstrafe**

Für jeden nachgewiesenen Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird die Zahlung einer Vertragsstrafe in Höhe von ..... € vereinbart.

## **12 Wirksamkeit der Vereinbarung**

Nebenabreden bedürfen der Schriftform.

Für den Fall, dass einzelne Bestimmungen dieses Vertrages unwirksam sein sollten, werden sie durch eine wirksame Vereinbarung ersetzt, die dem sich aus dem Vertragstext ergebenden Willen der Parteien am nächsten kommt. Die Wirksamkeit der Vereinbarung wird im übrigen hiervon nicht berührt.

Erfüllungsort und Gerichtsstand für alle sich aus oder im Zusammenhang mit diesem Vertrag stehenden Streitigkeiten ist der Geschäftssitz des Auftraggebers/Auftragnehmers.

Die beiderseitigen Verpflichtungen aus diesem Vertrag gehen auf den jeweiligen Rechtsnachfolger der Vertragspartei über.

# Anlage

## Datensicherungsmaßnahmen gemäß Zi. 7 des Vertrages<sup>8</sup>

Zum Schutz der Daten, die der Auftragnehmer im Rahmen dieses Vertrages für den Auftraggeber verarbeitet legen die Parteien folgende technische und organisatorische Maßnahmen verbindlich fest:<sup>9</sup>

### 1. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

---

---

---

---

### 2. Zugangskontrolle<sup>10</sup>

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

---

---

---

---

### 3. Zugriffskontrolle<sup>11</sup>

Maßnahmen, um zu gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

---

---

---

---

---

<sup>8</sup> Rechtsgrundlage ist für den Auftraggeber § 6 KDO, für den Auftragnehmer § 9 BDSG

<sup>9</sup> Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Ist das der Fall, sollte es zum Bestandteil dieses Vertrages gemacht werden. Auf das hier vorgeschlagene Formular kann dann verzichtet werden.

<sup>10</sup> Die Anmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.

<sup>11</sup> Besonders wichtig ist die Festlegung von Verantwortlichkeiten. Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.

#### 4. Weitergabekontrolle<sup>12</sup>

Maßnahmen, um zu gewährleisten dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert, oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

-----  
-----  
-----  
-----

#### 5. Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

-----  
-----  
-----  
-----

#### 6. Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

-----  
-----  
-----  
-----

#### 7. Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

-----  
-----  
-----  
-----

---

<sup>12</sup> Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten zu verschlüsseln.

8. Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

---

---

---

---