Der Diözesandatenschutzbeauftragte
des Erzbistums Hamburg,
der Bistümer Hildesheim, Osnabrück und des
Bischöflich Münsterschen Offizialats in Vechta i.O.

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Mustervertrag zur Fernwartung

(MV 803 - Stand: 07.04.2011)

Vorbemerkung:

Der nachfolgende Mustervertrag beinhaltet Regelungen zu datenschutzrelevanten Sachverhalten bei Hardware-Diagnosen und Software-Wartungsarbeiten, die nicht vor Ort, sondern im Wege des Fernzugriffs über das Internet erbracht werden. Es liegt auf der Hand, dass solche Verfahren mit besonderen Risiken verbunden sind. Er soll es daher kirchlichen Stellen erleichtern, mit den Auftragnehmern ausreichende vertragliche Regelungen unter Beachtung von § 6 der Anordnung über den kirchlichen Datenschutz - KDO - zu vereinbaren. Dabei kann der Inhalt des Vertrages jeweils aufgabenspezifisch angepasst werden. Das sollte allerdings nicht dazu führen, dass das hier angestrebte Schutzniveau unterschritten wird.

Eine Fernwartung ist ein Spezialfall der Datenverarbeitung im Auftrag im Sinne von § 8 KDO. Soweit spezialgesetzliche Regelungen für die Daten Anwendung finden, ist zunächst zu prüfen, ob eine Fernwartung überhaupt zulässig ist. Gegebenenfalls sind diese Regelungen bei der Vertragsgestaltung (z.B. Personal-, Beihilfe- und Sozialdaten) zu berücksichtigen. An nicht-kirchliche Stellen darf ein Auftrag zur Fernwartung nur vergeben werden, wenn weder gesetzliche Regelungen über besondere Berufs- oder Amtsgeheimnisse noch überwiegende schutzwürdige Belange der Betroffenen entgegenstehen. Die jeweiligen Vertragsbestimmungen sind dem Mustervertrag zu entnehmen.

Das hier vorgestellte Mustervereinbarung folgt einer Empfehlung des Hessischen Datenschutzbeauftragten[1] und wurde entsprechend den kirchlichen Vorschriften angepasst.

Hannover, den 07. April 2011

1 siehe: www.datenschutz.hessen.de/mustervertrag_fernwartung.htm#entry2153

Vereinbarung

zwischen dem/der

_____

(nachstehend Auftragnehmer genannt)

und dem/der

_____

(nachstehend Auftraggeber genannt)

§ 1 Gegenstand der Vereinbarung

Diese Vereinbarung umfasst folgende, vom Auftragnehmer durchzuführende Fernwartungsarbeiten:[2]

1. Hardware- Diagnose: für folgende Hardwareprodukt(e)
2. Software-Wartung: für folgend(e) Softwareprodukt(e)

§ 2 Verfahrensregelungen

(1) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind schriftlich zu vereinbaren.

(2) Mitteilungen der Vertragsparteien über E-Mail oder Internet werden nur akzeptiert, wenn das Schriftstück verschlüsselt übertragen wurde und mit einer digitalen Signatur versehen worden ist.

§ 3 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Fernwartung sowie für die Wahrung der Rechte der Betroffenen bleibt der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der Fernwartung 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 wird

2 Hinweis: Hier sind Art und Umfang der durchzuführenden Fernwartungsarbeiten, die davon betroffenen EDV-Systeme und Daten genau zu beschreiben. Beispielsweise könnte eine Hardware-Diagnose zur Vorbereitung einer Wartung erfolgen oder die Wartung einer Anwendungssoftware.

Beispiel: *"2. Software-Wartung:*
Behebung von Fehlerzuständen in der Anwendung xyz in der Abteilung N.
Damit verbunden sind folgende Zugriffe:
Schreibender Zugriff auf die Konfigurationsdateien ..... der Anwendung xyz.
Lesender Zugriff auf die anderen Dateien im Programmverzeichnis ..... der Anwendung xyz
Lesender Zugriff auf die Anwendungsdaten in den Verzeichnissen .....
Ein Zugriff auf die Datei ..... wird soweit erforderlich nach Rücksprache ermöglicht."

dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitgeteilt.

(3) Im System des Auftraggebers werden alle Zugriffe, die für Wartungsarbeiten erfolgen, protokolliert. Die Protokollierung muss so erfolgen, dass sie in einer Revision nachvollzogen werden kann. Die Protokollierung darf vom Auftragnehmer nicht abgeschaltet werden.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten feststellt, die bei der Fernwartung aufgetreten sind oder die einen Zugriff durch Unbefugte möglich machen.

(5) 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 zur Kenntnis zu bringen.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer führt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Er verwendet Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, nur für Zwecke der Fernwartung. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht 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 zur Kenntnis zu bringen.

(3) Der Auftragnehmer sichert die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(4) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen.

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

(6) Der Beginn der Fernwartung ist telefonisch anzukündigen, um den Beauftragten des Auftraggebers die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen.

(7) Fernwartungen dürfen nur von der Wartungszentrale aus vorgenommen werden, deren Sicherheitsmaßnahmen in § 7 Abs. 1 vereinbart worden sind.

(8) Der Auftragnehmer erkennt an, 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. Ergeben sich Zweifel, so gestattet der Auftragnehmer die Begehung der Räume, von denen aus die Fernwartung durchgeführt wird.

(9) Die Fernwartung von Privatwohnungen aus ist nicht gestattet. Soll im Einzelfall davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers. In diesem Fall 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.

(10) Wurden Daten des Auftraggebers im Zuge der Fernwartung kopiert, so sind diese nach Abschluss der konkreten Fernwartungsmaßnahme unverzüglich zu löschen. Dies gilt nicht

für Daten, die zur Dokumentationskontrolle und für Revisionsmaßnahmen der Fernwartung benötigt werden.

(11) Nicht mehr benötigte Unterlagen und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.[3]

(12) Die Einschaltung von Subauftragnehmern ist ausgeschlossen. Soll im Einzelfall davon abgewichen werden, bedarf dies der gesonderten schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer hat in diesem Falle vertraglich sicher zu stellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 5 erfüllt hat.

(13) Soweit für den Auftragnehmer die Vorschriften über den nichtöffentlichen Bereich Anwendung finden, bestätigt er, dass er gem. § 4 d Abs. 1 BDSG zum Register bei der Aufsichtsbehörde für den Datenschutz gemeldet ist oder gem. § 4 f BDSG einen betrieblichen Datenschutzbeauftragten bestellt hat.

(14) Für die Sicherheit erhebliche Entscheidungen zur Organisation und Durchführung der Fernwartung sind mit dem Auftraggeber abzustimmen.

(15) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, insbesondere wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird. Die Unterbrechung kann erfolgen, wenn eine Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten festgestellt wird.

§ 5 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, das Datengeheimnis gemäß § 4 KDO zu wahren. Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften; im Fall des § 4 Abs. 12 S.2 gilt das auch gegenüber dem Subunternehmer.

(3) Auskünfte an Dritte darf der Auftragnehmer nicht erteilen, Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen (§ 3 Abs. 2) erteilen.

§ 6 Kontrollrechte des Diözesandatenschutzbeauftragten

(1) Der Auftragnehmer verpflichtet sich, dem Diözesandatenschutzbeauftragten des (Erz-)Bistums _____ Zugang zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe des KDO in ihrer jeweiligen Fassung. Er benachrichtigt den Auftraggeber, bevor eine angekündigte Kontrolle statt findet.

(2) Soweit Daten in einer Privatwohnung verarbeitet werden, ist das Zugangsrecht für den Diözesandatenschutzbeauftragten vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer stellt sicher, dass die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

---

3 Hinweis: Für Beweissicherung, Auskunftsansprüche oder die Revision relevant

§ 7 **Datensicherungsmaßnahmen** (Erläuterungen im Anhang)

(1) Für die Zwecke der Vorabkontrolle des Auftragnehmers nach § 8 Abs. 2 Satz 3 KDO werden folgende technische und organisatorische Maßnahmen für die Fernwartungszentrale verbindlich festgelegt:

a) Zutrittskontrolle
Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:
.....
.....
b) Benutzerkontrolle
Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen und –verfahren gehindert werden:
.....
.....
c) Zugriffskontrolle
Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:
.....
.....
d) Datenverarbeitungskontrolle
Maßnahmen, damit personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden:
.....
.....
e) Verantwortlichkeitskontrolle
Maßnahmen, damit es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind:
.....
.....
f) Dokumentationskontrolle
Maßnahmen, damit durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der Datenverarbeitungsanlage und des -verfahrens möglich ist:
.....
.....
g) Organisationskontrolle
Maßnahmen, damit die innerbehördliche oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:
.....
.....
(2) Um die Übertragung der Daten abzusichern und unbefugte Zugriffe auf die Rechner des Auftraggebers im Rahmen der Fernwartung zu verhindern, legt der Auftraggeber folgende technische und organisatorische Maßnahmen für beide Seiten verbindlich fest:

a) Zutrittskontrolle[4]
Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:
.....

b) Benutzerkontrolle[5]
Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen und –verfahren gehindert werden:
.....

c) Zugriffskontrolle[6]
Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:
.....

d) Datenverarbeitungskontrolle[7]
Maßnahmen, damit personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden:
.....

e) Verantwortlichkeitskontrolle[8]
Maßnahmen, damit es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden

4 Hinweis: In den meisten Fällen werden im Zusammenhang mit der Fernwartung keine Maßnahmen zur Zutrittskontrolle getroffen. Es ist aber denkbar, dass der Auftragnehmer die Hardwarekomponenten (Router etc.) installiert und betreut. In diesem Fall sollten hier die Maßnahmen beschrieben werden, wann Wartungspersonal wie Zutritt zur Hardware erhält.

5 Hinweis: Hier sind insbesondere die Maßnahmen festzulegen, mit denen sichergestellt wird, dass die Fernwartung nur mit Wissen und Willen des Auftraggebers stattfindet und die Identität des Wartungspersonals festgestellt wird.

Beispiele:

Vor einer Wartung wird das Modem durch einen berechtigten Mitarbeiter des Auftraggebers aktiviert. Es wird eine Benutzerkennung für das Wartungspersonal eingerichtet. Um die Wartung durchführen zu können, muss die Kennung mit dem Passwort eingegeben werden. Es wird ein durch Chipkarten unterstütztes Challenge-Response-Verfahren zur Identifizierung des Wartungspersonals eingesetzt.

6 Hinweis: In § 1 des Vertrags ist der Umfang der Fernwartung festgelegt. Entsprechend dem Auftrag müssen die Zugriffsregeln für das Wartungspersonal definiert werden. Ein Zugriff auf andere Anwendungen oder Daten muss ausgeschlossen werden. Auch sind dem Wartungspersonal grundsätzlich keine Administratorrechte einzuräumen. Änderungen im Betriebssystem oder systemnaher Software sollten nur von Mitarbeitern des Auftraggebers vorgenommen werden, damit der Auftraggeber den Überblick über den Stand des Systems behält. Dies gilt umso mehr, wenn mehrere Anwendungen auf einem Rechner laufen und Änderungen im System während der Fernwartung die anderen Anwendungen beeinflussen würden.

Beispiel: Entsprechend dem Auftragsumfang werden die Zugriffsrechte des Wartungspersonals vergeben.

7 Hinweis: Die vorgesehen Maßnahmen müssen u.a. gewährleisten, dass die Verbindung nur zwischen der Wartungszentrale und den zu wartenden Rechnern aufgebaut werden kann. Außerdem dürfen Dritte die übertragenen Daten nicht zur Kenntnis nehmen können.

Beispiele: Die Datenübertragung wird verschlüsselt. Es kommt das Verfahren xyz zum Einsatz. Durch Call-Back-Verfahren wird die Verbindung zur Fernwartungszentrale aufgebaut

8 Hinweis: Die Protokollierung ist hier vor allem als Maßnahmen zu nennen. Um die Daten mit einem vertretbaren Aufwand auswerten zu können, müssen in der Regel Tools vorhanden sein.

Beispiele: Die Bildschirmanzeige des Wartungspersonals wird auf einer Konsole beim Auftraggeber gespiegelt.

Die übertragenen Daten werden protokolliert.

sind:
.....

f) Dokumentationskontrolle
Maßnahmen, damit durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der Datenverarbeitungsanlage und des -verfahrens möglich ist:
.....
.....
g) Organisationskontrolle[9]
Maßnahmen, damit die innerbehördliche oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:
.....

(3) Der Auftragnehmer beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.
(4) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.
(5) Unvorhergesehene Abweichungen von Abs. 1 hat der Auftragnehmer unverzüglich mitzuteilen. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.
(6) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei Fernwartung. Er unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber 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 ausdrücklich bestätigt wird.

§ 8 Vertragsdauer

(1) Der Vertrag beginnt am _____ und endet am _____/ (mit Auftragserledigung) / (wird auf unbestimmte Zeit geschlossen).
Er ist mit einer Frist von _____ Monaten zum Quartalsende kündbar.
(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des HDSG oder dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder des Hessischen Datenschutzbeauftragten vertragswidrig verweigert.

§ 9 Vergütung
....

§ 10 Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung

9 Hinweis: Hier können Schulungsmaßnahmen und die Revision des Verfahrens der Fernwartung festgelegt werden.

der vertraglichen Leistung schuldhaft verursachen.
(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem HDSG 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

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

§ 12 Nichterfüllung der Leistung

....

§ 13 Sonstiges

(1) Sollten 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.
(2) Für Nebenabreden ist die Schriftform erforderlich.
(3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen[10]

§ 14 Wirksamkeit der Vereinbarung

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

10 Hinweis: Diese Klausel muss wegen § 11 Nr. 2 AGB gesondert vereinbart werden.

Erläuterungen zu § 7 Datensicherungsmaßnahmen

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind.

Rechtsgrundlage ist § 8 Abs. 2 KDO, in dem beschrieben ist, welche Prüfungen ein Auftraggeber vor einer Auftragsvergabe durchzuführen hat. So muss der Auftragnehmer unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Auch hat der Auftraggeber zu prüfen, ob beim Auftragnehmer die nach § 6 KDO erforderlichen Maßnahmen getroffen werden.

Werden personenbezogene Daten bei der Fernwartung zur Kenntnis genommen, deren Verarbeitung für die Betroffenen keine besonderen Risiken erwarten lässt, so bietet das Grundschutzhandbuch des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen. (Das Handbuch, in dem die Maßnahmen erläutert werden, kann auf Datenträgern beim BSI bestellt werden.

a) Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Die Sicherheitsziele sind in der Anlage zu § 6 KDO (Zi. IV KDO-DVO) genannt. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte zum Vertragsbestandteil gemacht werden. In diesem Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen im Vertragstext zu wiederholen.

b) Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, das § 6 KDO genügt, müssen die einzelnen Maßnahmen im Vertrag gemeinsam festgelegt werden. Dabei sind wiederum die in der Anlage zu § 6 KDO genannten Sicherheitsziele zu erreichen. Entsprechend dem Katalog sind die einzelnen Maßnahmen in den Vertrag zu übernehmen. Es handelt sich um keinen abschließenden Maßnahmenkatalog. Insbesondere bei der Verarbeitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich.

c) Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

- V e r a n t w o r t l i c h k e i t e n: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.
- A b s c h o t t u n g: Es müssen Maßnahmen ergriffen werden, die ein unberechtigtes Eindringen in zu wartende Rechner soweit möglich verhindern. Dabei kann die Lösung vom einfachen Ausschalten des Modems bis zu technisch hochwertigen Challenge-Response-Verfahren gehen, die auf Chipkarten die geheimen Schlüssel speichern. Fallweise kann es nötig werden zu erkennen, ob und wie unberechtigte Personen versuchen einzudringen. Technische Komponenten, die dies feststellen können, sind Firewalls oder Intrusion Detection Systeme.
- A b h ö r e n d e r K o m m u n i k a t i o n: Zum Schutz gegen unberechtigtes Abhören sind die Daten, die bei der Fernwartung übertragen werden zu verschlüsseln.
- A n m e l d e p r o z e d u r e n: Die Anmeldung im System oder der zu wartenden Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.