

Vertrag zur Fernwartung

Der Vertrag für die Fernwartung gemäß § 11 Vereinbarung zwischen dem/der
I TRUST IT Computer Technik & Handel
nachstehend Auftragnehmer genannt
- und dem/der

.....
nachstehend Auftraggeber genannt

-

§ 1 Gegenstand der Vereinbarung

Diese Vereinbarung umfasst folgende, vom Auftragnehmer durchzuführende
Fernwartungsarbeiten:

1. Hardware - Diagnose: für folgende Hardwareprodukt(e)

- Diagnose zur Vorbereitung einer Wartung
- Wartung einer Anwendungssoftware.

2. Software - Wartung: für folgend(e) Softwareprodukt(e)

- 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...
- Ein Zugriff auf die Datei wird soweit erforderlich nach Rücksprache ermöglicht

§ 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 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, Dumps, Traces oder Debugger-Protokolle werden ohne Wissen des Auftraggebers nicht erstellt. Soweit möglich, erfolgt die Fernwartung am Bildschirm ohne gleichzeitige Speicherung.
- (2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Sachverhalte oder Unregelmäßigkeiten feststellt, die gegen das BDSG oder andere Vorschriften über den Datenschutz verstoßen insbesondere solche, die einen Zugriff durch Unbefugte möglich machen.
- (3) 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.
- (4) Der Auftragnehmer sichert die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.
- (5) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen.
- (6) 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.
- (7) Der Beginn der Fernwartung ist telefonisch anzukündigen, um den Beauftragten des Auftraggebers die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen.
- (8) Fernwartungen dürfen nur von der Wartungszentrale aus vorgenommen werden, deren Sicherheitsmaßnahmen in §7 Abs.1 vereinbart worden sind.
- (9) 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.
- (10) 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 Zutritt 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.
- (11) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen.

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

Hinweis: Für Beweissicherung, Auskunftsansprüche oder die Revision relevant

(13) 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.

(14) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren 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 zu wahren und die im Rahmen dieses Vertrages tätig werdenden Mitarbeiter auf das Datengeheimnis gemäß §5 BDSG schriftlich zu verpflichten. 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. 13 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.

(4) Der Auftragnehmer verpflichtet sich, bei der Fernwartung in sensiblen Bereichen, beispielsweise bei Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, nur fest angestellte Mitarbeiter für Fernwartungsarbeiten einzusetzen, die nach dem Verpflichtungsgesetz verpflichtet sind.

§ 6 Kontrollrechte der Aufsichtsbehörden

(1) Der Auftragnehmer verpflichtet sich, der für den Auftraggeber zuständigen Kontrollbehörde insbesondere den von dieser eingesetzten Bediensteten Zutritt zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe des § 38 BDSG in seiner jeweiligen Fassung.

(2) Soweit Daten in einer Privatwohnung verarbeitet werden, ist das Zugangsrecht für die Mitarbeiter der Aufsichtsbehörde und der von ihr eingesetzten Bediensteten vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer stellt sicher, dass die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

Hinweis: Bei öffentlichen Auftraggebern ist dieser Paragraf entsprechend des gültigen Bundes- oder Landesdatenschutzgesetzes zu modifizieren.

§ 7 Datensicherungsmaßnahmen

(1) 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) Maßnahmen, damit die innerbetriebliche (oder innerbehördliche) Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:

.....

Hinweis :

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

Vor allem ist die Dokumentation aller wesentlichen

Verarbeitungsschritte sowie der zur Fernwartung eingesetzten Hard- und Software zu vereinbaren, damit die Überprüfbarkeit möglich ist.

Die Protokollierung ist hier vor allem als Maßnahme 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.

b) Zutrittskontrolle

g) Trennungsgebot

Die Maßnahmen müssen gewährleisten, dass die zum Test der erfolgten Wartungsarbeiten bestimmten personenbezogenen Daten getrennt von den produktiven Datenbeständen verarbeitet werden können:

.....

Hinweis:

Nur im absoluten Ausnahmefall (nicht immer sind Testdaten für eine bestimmte Konstellation ausreichend!) sollte der Zugriff auf produktive Daten genehmigt werden.

Beispiel:

Beim Auftragnehmer wird eine Testumgebung eingerichtet, die der Realität beim Auftraggeber weitgehend entspricht. Der Auftraggeber stellt dafür eine Testdatenbank zur Verfügung und pflegt diese.

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

(3) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

(4) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen oder unvorhergesehen vom vereinbarten Standard abweichen, benachrichtigt er den Auftraggeber unverzüglich.

§ 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 BDSG oder dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der Aufsichtsbehörde 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 der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG 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) Der Auftragnehmer übereignet dem Auftraggeber zur Sicherung die Datenträger, auf denen sich Dateien befinden, die Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen und von anderen Datenbeständen getrennt zu halten.

(2) 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.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i.S.v. §273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen

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

§ 14 Wirksamkeit der Vereinbarung

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

Ort, Datum, Unterschriften

Erläuterungen zu § 7 Datensicherungsmaßnahmen

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind. Rechtsgrundlage ist §11 Abs.2 BDSG, 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 §9 BDSG 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).

Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. 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. Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, das §9 BDSG genügt, müssen die einzelnen Maßnahmen im Vertrag gemeinsam festgelegt werden. Es handelt sich um keinen abschließenden Maßnahmenkatalog. Insbesondere bei der Verarbeitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich.

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 wie 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.