

Vereinbarung zum Datenschutz

(Fernwartung, Umgang mit Kundendaten)

zwischen dem/der
michael martin GmbH & Co.KG
- nachstehend Auftragnehmer genannt -
und dem/Kunden
- nachstehend Auftraggeber genannt -

§ 1 Gegenstand der Vereinbarung

Diese Vereinbarung umfasst die vom Kunden beauftragte Dienstleistung und alle dazu zugehörigen Arbeiten an der Hardware, sowie der Software, insb. zu dem Bestimmungen des Datenschutzes.

§ 2 Verfahrensregelungen

Abweichungen zu dieser Vereinbarung sind immer schriftlich zu fixieren. Mündliche Abreden sind nicht gültig.

§ 3 Geheimhaltung von Daten

- (1) Der Auftragnehmer verpflichtet sich, das Datengeheimnis gemäß BDSG zu wahren. Er verpflichtet sich, die gleichen Geheimnischutzregeln zu beachten.
- (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; dies gilt 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 (§ 5 Abs. 6) erteilen.
- (4) Der Auftragnehmer verpflichtet sich auf gespeicherte Daten nur insoweit zuzugreifen, wie es die nachfolgenden Bestimmungen gestatten.
- (5) Sollten dem Auftragnehmer Inhalte von Datenbeständen bekannt werden, verpflichtet er sich, diese geheim zu halten.
- (6) Der Auftragnehmer verpflichtet sich, das eingesetzte Personal in der gleichen Weise zu verpflichten und die so begründeten Geheimhaltungspflichten zu überwachen.
- (7) Die Vergabe von Unteraufträgen ist nur mit Zustimmung des Auftraggebers zulässig.
- (8) Der Auftragnehmer sichert dem Auftraggeber zu, dass er nach Abschluss der Arbeiten alle Daten des Auftraggebers, die er während der Arbeiten kopiert oder ausgedruckt hat, unverzüglich löschen oder vernichten wird. Datenträger, die der Auftraggeber für die Arbeiten zur Verfügung gestellt hat, sind dem Auftraggeber unmittelbar nach Abschluss der Arbeiten wieder auszuhändigen.**

§ 4 Datensicherheit

- (1) Daten, die dem Auftragnehmer zur Verfügung gestellt werden, müssen immer beim Auftraggeber als überprüfte Sicherheitskopie vorhanden sein.
- (2) Der Auftraggeber sichert zu, dass vor Beginn der Dienstleistung eine aktuelle funktionsfähige Datensicherung vorhanden ist, so das im Schadensfalle auf diese zugegriffen werden kann.
- (3) Änderungen an Dateien, die im Zuge der Arbeiten erforderlich geworden sind, müssen vom Auftragnehmer dokumentiert werden.
- (4) Beim Austausch von Komponenten, mit denen Daten dauerhaft gespeichert werden können, insbesondere Festplattenlaufwerke und ähnliche Speichermedien, stellt der Auftragnehmer sicher,

dass entnommene Komponenten nach Abschluss der Arbeiten in einer Weise zerstört werden, die den Zugriff oder eine Wiederherstellung von Daten technisch ausschließt.

(5) Wünscht der Auftraggeber die Aushändigung von ausgetauschten Komponenten, sind diese bis zur Übergabe unter Verschluss zu halten.

§ 5 Pflichten des Auftraggebers bei Fernwartung

(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.

(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. Sollte die Protokollierung nicht gewünscht oder vorhanden sein, geht dies im Schadensfall zu Lasten des Auftraggebers. Der Auftragnehmer ist nicht verpflichtet die ordnungsgemäße Protokollierung zu überprüfen.

(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.

(6) Für die Fernwartung wird ausschließlich die in der Software zur Verfügung gestellte Funktion genutzt. Der Auftraggeber ist in der Lage, diese Funktion für einzelne Benutzer zu sperren. Sofern diese Funktion nicht gesperrt ist, kann der Auftragnehmer davon ausgehen, dass der Auftraggeber die Erlaubnis zur Fernwartung für diesen Mitarbeiter erteilt hat. Sollte die Nutzung des Programms und damit die Fernwartungsfunktion nicht möglich sein, teilt der Auftraggeber dem Auftragnehmer vor Beginn der Fernwartung schriftlich mit, welche Mitarbeiter er dafür einsetzen wird und wie diese Mitarbeiter sich identifizieren werden.

(7) Fernwartungen dürfen nur in die Geschäftsräume des Auftraggebers erfolgen. Der Auftraggeber muss bei Abweichung sofort den Auftragnehmer informieren und ggf. den Zugriff schriftlich erlauben. Sollte der Auftragnehmer nicht vom Auftraggeber informiert werden, haftet der Auftraggeber voll.

(8) Der Zugriff auf Computer in Privatwohnungen 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 Auftragnehmer vorher mit dem Auftraggeber abzustimmen. Es gelten die Informationspflichten aus §5 Abs 7. Der Auftraggeber sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(9) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, insbesondere wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird.

§ 6 Pflichten des Auftragnehmers bei Fernwartung

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

- (6) 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.
- (7) Nicht mehr benötigte Unterlagen und Dateien werden nach Abschluss der Dienstleistung datenschutzgerecht vernichtet.
- (8) **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.
- (9) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, insbesondere wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird.

§ 7 Datensicherungsmaßnahmen Allgemein

Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit der michael martin GmbH & Co.KG um das erforderliche Schutzniveau für die Erhebung, Verarbeitung und Nutzung von Sozialdaten zu gewährleisten

Angabe und Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit, die im Einzelfall getroffen wurden, um

- (a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
Alle Server sind in einem eigenen Serverraum untergebracht. Diese Tür ist grundsätzlich verschlossen und kann nur mit dem entsprechenden Schlüssel (elektronischer PIN) geöffnet werden.
- (b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
Der Zugriff auf die Computer kann nur nach einer erfolgreichen Authentifizierung innerhalb des Netzwerks erfolgen.
- (c) zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können,
Es ist sichergestellt, dass die Mitarbeiter nur Zugriff auf Daten haben, die sie für die Ausführung Ihrer Tätigkeit haben.
- (d) und dass Sozialdaten bei der Verarbeitung, Nutzung sowie nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
Alle Zugriffe werden vollständig protokolliert.
- (e) zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,
Alle Zugriffe werden vollständig protokolliert. Zudem erfolgt die elektronische Übertragung grundsätzlich verschlüsselt. Der Zugriff unterliegt den Bestimmungen von §7 (b)
- (f) und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Sozialdaten durch Einrichtungen der Datenübertragung vorgesehen ist (Weitergabekontrolle),
Alle Zugriffe werden vollständig protokolliert.
- (g) zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
Alle Zugriffe werden vollständig protokolliert
- (h) zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle),
Die Bearbeitung der Daten unterliegen den Bestimmungen dieses Datenschutzvertrages. Alle Mitarbeiter der michael martin GmbH & Co.KG haben von den Vorgehensweisen Kenntnis und sind explizit angewiesen dies umzusetzen.

(i) zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

Es erfolgt eine tägliche vollständige Datensicherung im Mehrgenerationenprinzip. Die Server sind gegen Stromausfall mit sog. USVs geschützt. Zudem sind die Festplatten der Server gegen Ausfall durch sog. RAID Systeme geschützt.

(j) zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können.

Die Verarbeitung unterliegt dem in §7 (c) definierten Zugriff. Die Daten werden getrennt in verschiedenen Anwendungen mit unterschiedlichen Zugriffsrechten gespeichert.

§ 8 Datensicherungsmaßnahmen der Fernwartung in Ergänzung zu §7

(1) Um die Übertragung der Daten abzusichern und unbefugte Zugriffe auf die Rechner des Auftraggebers im Rahmen der Fernwartung zu verhindern, legt der Auftragnehmer folgende technische und organisatorische Maßnahmen für beide Seiten verbindlich fest:

a) Zutrittskontrolle

keine

b) Benutzerkontrolle

Vor einer Wartung muss vom Auftraggeber das Programm Teamviewer aktiviert werden. Die Zugangsdaten werden von diesem Programm erzeugt und müssen telefonisch dem Auftragnehmer mitgeteilt werden. Der Auftraggeber stellt sicher, dass den Zugriff auf die Fernwartung nur autorisierte Mitarbeiter haben.

c) Zugriffskontrolle

Der Auftraggeber stellt sicher, dass der Benutzer, der das Fernwartungsprogramm starten darf, auch nur die Zugriffsrechte innerhalb der EDV Anlage besitzt, auf die auch der Auftragnehmer im Rahmen seiner Tätigkeit (§1) haben darf.

d) Datenverarbeitungskontrolle

Die gesamte Datenübertragung wird verschlüsselt.

Verschlüsselung: Das Fernwartungsprogramm arbeitet mit vollständiger Verschlüsselung auf Basis eines RSA Public-/Private Key Exchange und RC4 Session Encoding. Diese Technik wird auch bei https/SSL eingesetzt und gilt nach heutigem Standard der Technik als vollständig sicher. Da der Private Key niemals den Clientrechner verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Rechner im Internet den Datenstrom nicht entziffern können.

Zugangssicherung: Zusätzlich zur automatisch generierten PartnerID erzeugt das Fernwartungsprogramm ein dynamisches Sitzungskennwort, das sich in der Standardeinstellung bei jedem Start ändert und damit zusätzliche Sicherheit gegen unberechtigten Zugang zum System bietet. Wichtige Zusatzfunktionen wie der Dateitransfer erfordern eine zusätzliche, manuelle Bestätigung des Anwenders. Außerdem ist es generell nicht möglich, einen Rechner unbemerkt zu kontrollieren, da der Anwender am entfernten Rechner aus Datenschutzgründen über einen Zugriff informiert sein muss.

Codesignierung: Als zusätzliche Sicherheitsfunktion werden alle unsere Programme mittels VeriSign Code Signing signiert. Dadurch ist der Herausgeber der Software immer zuverlässig identifizierbar.

e) Verantwortlichkeitskontrolle

Der Auftraggeber stellt die vollständige Protokollierung sicher.

f) Dokumentationskontrolle

Der Auftraggeber stellt die vollständige Protokollierung sicher.

g) Organisationskontrolle

(1) Es wird immer die aktuelle Version des Fernwartungsprogramms eingesetzt. Dadurch wird sichergestellt, dass die Datenschutz- und Sicherungsmaßnahmen dem aktuellen Stand der Technik entsprechen.

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

(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) Unvorhergesehene Abweichungen hat der Auftragnehmer unverzüglich mitzuteilen. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.
- (5) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftragnehmer unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei Fernwartung. Der Auftraggeber unterrichtet den Auftragnehmer unverzüglich, wenn eine vom Auftragnehmer erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann.

§ 9 Dauer

- (1) Diese Vereinbarung gilt ab der Beauftragung und Endet mit der Kündigung des Softwarepflegevertrages.

§ 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 nur für Vorsatz oder grobe Fahrlässigkeit.
- (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.
- (3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, ist der Rückgriff beim Auftragnehmer ausgeschlossen.
- (4) Wird der Inhalt von Datenbeständen entgegen der Geheimhaltungspflichten Dritten bekannt, hat der Auftragnehmer den dadurch entstehenden Schaden zu ersetzen. Zum ersatzpflichtigen Schaden gehören auch Zahlungen, die der Auftraggeber Dritten zu leisten hat.
- (5) Den Nachweis für das Verschulden hat der Auftraggeber zu erbringen.
- (6) Für ein Verschulden ihres Personals haften Auftraggeber und Unterauftragnehmer in gleicher Weise wie für eigenes Verschulden.

§ 11 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

§ 12 Wirksamkeit der Vereinbarung

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