SOFTSTAR Computer Systems GmbH - Erdinger Str. 13 - 84416 Taufkirchen
Tel.: 08084/41330-0 - Fax: 08084/41330-33 - www.softstar.de

Vereinbarung zur Auftragsverarbeitung

Zwischen

Name:_____

_____

Straße:_____

PLZ / Ort: _____

Kd.-Nr. _____

(Auftraggeber)

und der

SOFTSTAR Computer Systems GmbH
Erdinger Straße 13
84416 Taufkirchen (Vils)

(Auftragnehmer)

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag zur Leistungserbringung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag zur Leistungserbringung in Zusammenhang stehen und bei denen Beschäftigte des *Auftragnehmers* oder durch den *Auftragnehmer* Beauftragte personenbezogene Daten (»Daten«) des *Auftraggebers* verarbeiten.

A) Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

(1) Art der Daten:
- Personenstammdaten
- Kommunikationsdaten
- Abrechnungs- und Zahlungsdaten
- Vertragsstammdaten
- Kundenhistorie
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, oder aus öffentlichen Verzeichnissen)

(2) Art und Zweck der Datenverarbeitung
- Wartung und Support (per Fernzugriff)
- Datenanalysen/-reparaturen/-bearbeitung (Datensicherungen)
- Individualisierungen
- Formular-/Layout Anpassungen

(3) Kategorien betroffener Personen
- Debitoren
- Interessenten
- Kreditoren
- Handelsvertreter
- Ansprechpartner

Die Laufzeit der Datenerfassung richtet sich nach der Vertragslaufzeit, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

B) Anwendungsbereich und Verantwortlichkeit

(1) Der *Auftragnehmer* verarbeitet personenbezogene Daten im Auftrag des *Auftraggebers*. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der *Auftraggeber* ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den *Auftragnehmer* sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom *Auftraggeber* danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom *Auftragnehmer* bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

C) Pflichten des Auftragnehmers

(1) Der *Auftragnehmer* darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des *Auftraggebers*, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor, verarbeiten. Der *Auftragnehmer* informiert den *Auftraggeber* unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der *Auftragnehmer* darf die Umsetzung der Weisung solange aussetzen, bis sie vom *Auftraggeber* bestätigt oder abgeändert wurde.

(2) Der *Auftragnehmer* wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des *Auftraggebers* treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der *Auftragnehmer* hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem *Auftraggeber* sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem *Auftragnehmer* vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Die aktuell eingesetzten technischen und organisatorischen Maßnahmen können jederzeit auf der Webseite des *Auftragnehmers* unter nachfolgendem Link eingesehen werden. http://softstar.de/datenschutz.html

(3) Der *Auftragnehmer* unterstützt soweit vereinbart den *Auftraggeber* im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(4) Der *Auftragnehmer* gewährleistet, dass es den mit der Verarbeitung der Daten des *Auftraggebers* befassten Mitarbeiter und andere für den *Auftragnehmer* tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der *Auftragnehmer*, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der *Auftragnehmer* unterrichtet den *Auftraggeber* unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des *Auftraggebers* bekannt werden. Der *Auftragnehmer* trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem *Auftraggeber* ab.

(6) Der *Auftragnehmer* nennt dem *Auftraggeber* den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
Der Datenschutzbeauftragter des Auftragnehmers ist auf folgender Seite http://softstar.de/datenschutz.html zu entnehmen.

(7) Der *Auftragnehmer* gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der *Auftragnehmer* berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der *Auftraggeber* dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der *Auftragnehmer* die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den *Auftraggeber* oder gibt diese Datenträger an den *Auftraggeber* zurück, sofern nicht im Vertrag bereits vereinbart.
In besonderen, vom *Auftraggeber* zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe; Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des *Auftraggebers* entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der *Auftraggeber*.

(10) Im Falle einer Inanspruchnahme des *Auftraggebers* durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der *Auftragnehmer* den *Auftraggeber* bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

D) Pflichten des Auftraggebers

(1) Der *Auftraggeber* hat den *Auftragnehmer* unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des *Auftraggebers* durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der *Auftraggeber* nennt auf Seite 5 des Vertrags dem *Auftragnehmer* den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

E) Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den *Auftragnehmer*, wird der *Auftragnehmer* die betroffene Person an den *Auftraggeber* verweisen, sofern eine Zuordnung an den *Auftraggeber* nach Angaben der betroffenen Person möglich ist. Der *Auftragnehmer* leitet den Antrag der betroffenen Person unverzüglich an den *Auftraggeber* weiter. Der *Auftragnehmer* unterstützt den *Auftraggeber* im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der *Auftragnehmer* haftet nicht, wenn das Ersuchen der betroffenen Person vom *Auftraggeber* nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

F) Nachweismöglichkeiten

(1) Sollten im Einzelfall Inspektionen durch den *Auftraggeber* oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs, nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der *Auftragnehmer* darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den *Auftraggeber* beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem *Auftragnehmer* stehen, hat der *Auftragnehmer* gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der *Auftragnehmer* eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den *Auftragnehmer* grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(2) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des *Auftraggebers* eine Inspektion vornehmen, gilt grundsätzlich Absatz 1 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

G) Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der *Auftraggeber* vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der *Auftragnehmer* weitere *Auftragnehmer* mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der *Auftragnehmer* wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift der/des Subunternehmer/s:

.....

.....

Beschreibung der Teilleistungen:

.....

.....

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer informiert der *Auftragnehmer* den *Auftraggeber*. Der *Auftraggeber* kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom *Auftraggeber* bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.

(4) Erteilt der *Auftragnehmer* Aufträge an Subunternehmer, so obliegt es dem *Auftragnehmer*, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

(5) Unter bestimmten Umständen müssen Daten an Dritte weitergegeben werden.
Beispiele: Lizenzbestellung für den Kunden
Produktregistrierung beim Hersteller
Aktivierung des Support-Packs (Garantieerweiterung)

In der Regel geht es um Folgende Angaben: Firmenname, Anschrift, Kontaktdaten und Ansprechperson beim Kunden.

H) Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des *Auftraggebers* beim *Auftragnehmer* durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der *Auftragnehmer* den *Auftraggeber* unverzüglich darüber zu informieren. Der *Auftragnehmer* wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim *Auftraggeber* als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des *Auftragnehmers* – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

I) Haftung und Schadensersatz

(1) Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.

(2) Soweit keine Haftungsregelung vereinbart wurde, haften *Auftraggeber* und *Auftragnehmer* gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Taufkirchen (Vils), den _____ _____, den _____

_____ _____
SOFTSTAR Computer Systems GmbH rechtskräftige Unterschrift Auftraggeber

Name und Position des Ansprechpartners für Datenschutzfragen gemäß **Punkt D) Nr. 3** des Vertrags:

_____

_____

Anlage 1

Technisch-organisatorische Maßnahmen (TOM's)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, durch Schlüsselkonzepte
Zugangskontrolle
Keine unbefugte Systembenutzung, durch sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Firewall;
Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. durch Mandantenfähigkeit, Sandboxing;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, durch Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/ offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.