Vereinbarung gemäß § 11 BDSG zur Auftragsdatenverarbeitung

Vereinbarung

zwischen

Worldsoft AG
Churerstrasse 158
8808 Pfäffikon SZ
Schweiz

- nachstehend Auftragnehmer genannt -

und

Name, Vorname	Firma
Straße,Nr.	Land,PLZ,Ort

– nachstehend Auftraggeber genannt –

1. Gegenstand und Dauer des Auftrags

1.1. Der Gegenstand des Auftrags ergibt sich aus der aktuellen Leistungsvereinbarung, auf die hier verwiesen wird (im folgenden Leistungsvereinbarung). Diese ist einsehbar unter: http://www.worldsoft.info/bestellen. Änderungen der Leistungsvereinbarung lassen diese Vereinbarung zur Auftragsdatenverarbeitung unberührt, sofern infolge solcher Änderungen nicht strengere Anforderungen an diese zu stellen sind.

1.2. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung (Abonnement bei Worldsoft).

2. Konkretisierung des Auftragsinhalts

2.1. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Datenschutzerklärung und Datensicherheits-beschreibung des Auftragnehmers. Diese sind einsehbar unter: http://www.worldsoft.info/datenschutz und http://www.worldsoft.info/datensicherheit. Änderungen der Datenschutzerklärung und Datensicherheitsbeschreibung lassen diese Vereinbarung zur Auftragsdatenverarbeitung unberührt, sofern infolge solcher Änderungen nicht strengere Anforderungen an diese zu stellen sind.

2.2. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Schweiz, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

2.3. Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien: Personenstammdaten, Bestandsdaten, Nutzungsdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie und je nach den verwendeten Modulen auch Rechnungsinformationen, Provisionsabrechnungen und Bankverbindungen.

2.4. Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst Kunden, Interessenten und Abonnenten.

3. Rechte und Pflichten des Auftraggebers

3.1. Der Auftraggeber ist verantwortliche Stelle (§ 3 Abs. 7 BDSG) für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber. Dem Auftragnehmer steht das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitung hinzuweisen.

3.2. Der Auftraggeber ist als verantwortliche Stelle für die Wahrung der Betroffenenrechte verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

3.3. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen.

3.4. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

3.5. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach § 42a BDSG besteht, ist der Auftraggeber für die Erfüllung der Pflichten aus § 42a BDSG verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder der Leistungsbeschreibung des Auftragnehmers für die entsprechende Dienstleistung. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

4.2. Der Auftragnehmer bestätigt, dass er, soweit gesetzlich erforderlich, einen betrieblichen Datenschutzbeauftragten i.S.d. § 4f BDSG bestellt hat und wird diesen gegenüber dem Auftraggeber schriftlich oder in Textform (z.B. E-Mail) benennen.

4.3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

4.4. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

4.5. Der Auftragnehmer ist zur Wahrung des Datengeheimnisses entsprechend § 5 BDSG verpflichtet. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

4.6. Der Auftragnehmer ist zur Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags verpflichtet.

4.7. Der Auftragnehmer ist zur Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber verpflichtet. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutz-auditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

5. Kontrollrechte des Auftraggebers

5.1. Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

5.2. Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Für die Aufwände, die der Auftragnehmer bei der Durchführung von Kontrollmaßnahmen hat, werden dem Auftraggeber pauschal pro Stunde 300 Euro zzgl. USt. in Rechnung gestellt.

6. Mitteilung bei Verstößen des Auftragnehmers

6.1. Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

6.2. Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

7. Weisungsbefugnis des Auftraggebers

7.1. Der Auftragnehmer bietet standardisierte, webbasierte Softwareprogramme mit fest definierten Funktionalitäten, die je nach gebuchtem Paket freigeschaltet werden. In diesem Rahmen hat der Auftraggeber die Möglichkeiten, die Datenverarbeitung vollumfänglich selbst zu steuern (Weisungserteilung). Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Erteilung der Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen innerhalb seines Benutzerkontos bei Worldsoft, z.B. durch entsprechende Konfiguration, konkretisieren kann. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

7.2. Weisungen wird der Auftraggeber durch die Einstellungsmöglichkeiten innerhalb seines Benutzerkontos bei Worldsoft erteilen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

7.3. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

8. Löschung von Daten und Rückgabe von Datenträgern

8.1. Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Hierzu räumt der Auftragnehmer dem Auftraggeber die Möglichkeit ein, über sein Benutzerkonto bei Worldsoft sämtliche Daten zu exportieren. Macht er von dieser Möglichkeit keinen Gebrauch, so werden diese Daten datenschutzgerecht vernichtet. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

8.2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

9. Technisch-organisatorische Maßnahmen

9.1. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

9.2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

10. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

11. Unterauftragsverhältnisse

11.1. Der Auftragnehmer bedient sich Unterauftragnehmern wie beispielsweise Rechenzentrumsbetreibern, Softwareentwicklern und Systemadministratoren. Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden müssen, wird dies hiermit durch den Auftraggeber genehmigt.

11.2. Der Auftragnehmer verpflichtet sich bei der Auswahl seiner Unterauftragnehmer zur Einhaltung der folgenden Anforderungen:

- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so gestaltet, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Bei der Unterbeauftragung hat der Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer eingeräumt. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

11.3. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

12. Schlussbestimmungen

12.1 Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

12.2. Für Nebenabreden ist die Schriftform erforderlich.

12.3. Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.

12.4. Soweit zulässig, vereinbaren die Parteien den Gerichtsstand am Sitz des Auftragnehmers.

.....
Ort, Datum

.....
Unterschrift Auftraggeber

.....
Ort, Datum

.....
Unterschrift Auftragnehmer

Allgemeine technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage

1. Zutrittskontrolle

Der unbefugte Zutritt wird verhindert, indem technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten, getroffen worden sind:

- Protokollierung der Besucher
- Zutrittskontrollsysteme (Ausweisleser, Magnetkarte, Chipkarte)
- Türsicherung (elektrische Türöffner usw.)
- Werkschutz, Pförtner
- Überwachungseinrichtung: Alarmanlage, Video- / Fernsehmonitor

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme wird verhindert, indem technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung getroffen worden sind:

- Passwortvergabe (Benutzername und Passwort)
- Zuordnung von Benutzerprofilen
- Protokollierung der Benutzer
- Verschlüsselung von Datenträgern

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden verhindert, indem das Berechtigungskonzept und die Zugriffsrechte sowie deren Überwachung und Protokollierung bedarfsgerecht ausgestaltet worden sind:

- Differenzierte Berechtigungen der Benutzer (Profile, Rollen, Transaktionen und Objekte)
- Passwortrichtlinie inklusive Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Anzahl der Administratoren auf das „Notwendigste“ reduziert

4. Weitergabekontrolle

Bei der Weitergabe personenbezogener Daten (manueller bzw. elektronischer Transport, Übertragung, Übermittlung oder Speicherung auf Datenträger) sowie bei der nachträglichen Überprüfung wurden die folgenden Maßnahmen getroffen:

- Verschlüsselung
- Übermittlungskontrolle
- Protokollierung

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist gewährleistet. Hierzu wurden Protokollierungssysteme implementiert, mit denen nachträglich überprüft werden kann, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist gewährleistet. Hierzu wurden technische und organisatorische Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer getroffen. Hierzu zählen:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust geschützt. Hierzu wurden die folgenden physikalischen und logischen Maßnahmen zur Datensicherung getroffen:

- Klimaanlagen in Serverräumen
- 24/7 Überwachung der Geräte
- Backup-Verfahren
- Spiegeln der Daten in ein zweites Datencenter
- Stromversorgung mit Diesel und USV
- Umfassender Brandschutz
- Virenschutz / Firewall

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet. Hierzu wurden die folgenden Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken getroffen:

- Berechtigungskonzept
- Logische Mandantentrennung (softwareseitig)
- Versehen der Datenfelder mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem