Vertrag für die Auftragsdatenverarbeitung

Firma	Name, Vorname des Ansprechpartners für Datenschutzfragen
Straße, Nr.	Land, PLZ, Ort

– nachstehend Auftraggeber genannt –

und

Worldsoft AG
Churerstrasse 158, 8808 Pfäffikon SZ, Schweiz
Ansprechpartner für Datenschutzfragen: Gert Friedrich Lang

- nachstehend Auftragnehmer genannt -

1. Einleitung, Geltungsbereich, Definitionen

1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer im Rahmen einer Verarbeitung personenbezogener Daten im Auftrag.

1.2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Mit Begriffen wie „Datenverarbeitung" oder „Verarbeitung" wird die Verwendung von personenbezogenen Daten verstanden.

2. Gegenstand und Dauer der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst Webhostingleistungen im Rahmen der vom Auftragnehmer auf dessen Websites angebotenen und in den jeweiligen Leistungsbeschreibungen konkretisierten Produkten. Änderungen der Leistungsvereinbarung lassen diesen Vertrag zur Auftragsdatenverarbeitung unberührt, sofern infolge solcher Änderungen nicht strengere Anforderungen an diese zu stellen sind.

3. Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

3.1. Art und Zweck der Verarbeitung

Die Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung, Anonymisieren, Pseudonymisieren, Verschlüsseln oder sonstige Nutzung von Daten.

Folgende Datenarten/-kategorien sind Gegenstand der Datenverarbeitung: Adressdaten, Stammdaten, Mitarbeiterdaten, Bestandsdaten, Nutzungsdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsdaten, Abrechnungsdaten, Bankverbindungsdaten, Bestelldaten, E-Mail-Nachrichten, Kundenhistorie, Dateien (PDF), Videos und Bilder.

3.2. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind Kunden, Nutzer, Lieferanten, Interessenten, Mitarbeiter, Bewerber, Geschäftspartner, Mitglieder, Dienstleister, Praktikanten und Abonnenten.

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. 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.

4.2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer hat technische und organisatorische Maßnahmen getroffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung sicherstellen. Der Auftragnehmer überprüft regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und passt die Maßnahmen nötigenfalls an. Diese aktuellen Maßnahmen sind in Anhang 1 dieses Vertrages beschrieben.

4.3. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt 33 bis 36 DS-GVO genannten Pflichten. Die dadurch begründeten Kosten sind vom Auftraggeber zu tragen.

4.4. 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.

4.5. 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 Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

4.6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

4.7. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

4.8. Der Auftragnehmer kann dem Auftraggeber Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

4.9. 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. Die dadurch begründeten Kosten sind vom Auftraggeber zu tragen.

4.10. Die Auftragsverarbeitung erfolgt in der Schweiz oder innerhalb der EU. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen. Für die Schweiz gilt ein dem EU-Recht vergleichbares Datenschutzniveau und eine Datenübermittlung in die Schweiz ist datenschutzrechtlich zulässig.

5. Rechte und Pflichten des Auftraggebers

5.1. 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).

5.2. Der Auftraggeber ist als verantwortliche Stelle für die Wahrung der Betroffenenrechte verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §4 Abs. 10 dieses Vertrages entsprechend.

5.3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5.4. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung schriftlich zu erteilen. Nach Beendigung des Hauptvertrages werden sämtliche Daten gelöscht. Es obliegt dem Auftraggeber, Daten vor Beendigung des Vertrages umzuziehen beziehungsweise eine Sicherungskopie anzufertigen. Der Auftraggeber hat selbst Zugriff auf seine Daten, insofern trifft den Auftragnehmer keine Pflicht zur Herausgabe. Die Obliegenheit des Auftraggebers zur Datensicherung während der Vertragslaufzeit bleibt hiervon unberührt.

6. Wahrung von Betroffenenrechten

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.

7. Nachweismöglichkeiten

7.1. Auftraggeber und Auftragnehmer verständigen sich darauf, dass der Nachweis für die Einhaltung der Pflichten aus diesem Vertrag durch Veröffentlichung von Informationen erbracht wird, die auf der gleichen Worldsoft-Webseite wie dieser Vertrag zu finden sind:

- Datenschutzerklärung für Provider-Dienstleistungen
- Informationen zur Datensicherheit
- PDF über den Datenfluss der Worldsoft Business Suite

7.2. 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.

Die Kosten für beauftragte Prüfer trägt der Auftraggeber. Für die Unterstützung bei der Durchführung einer Inspektion vergütet der Auftraggeber dem Auftragnehmer die Kosten für die entstehenden Aufwendungen.

7.3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 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.

8. Subunternehmen

8.1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

8.2. 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.

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

9. Vertragslaufzeit

Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Sollten Leistungen auch noch nach Beendigung des Hauptvertrages erbracht werden, gilt dieser Vertrag auch für diese weitere Leistungserbringung für die gesamte Dauer der tatsächlichen Leistungserbringung.

10. Haftung und Schadenersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

11. Sonstiges

11.1. Sollte Eigentum 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 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.

11.2. Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform.

11.3. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

.....	Pfäffikon, 13. April 2018
Ort, Datum	Ort, Datum
.....	.....
Unterschrift Auftraggeber	Unterschrift Auftragnehmer vertreten durch Gert F. Lang, CEO, Worldsoft AG

Anlage: Technische und organisatorische Maßnahmen

1. Zutrittskontrolle

Der unbefugte Zutritt zur Server-Plattform 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
- 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