

Vertrag zur Auftragsverarbeitung (AV) nach Art. 28 Abs. 3 DS-GVO

zwischen der

KaiTech IT-Systems GmbH
Im Döreener Feld 2
33100 Paderborn

(nachfolgend „Auftragnehmer“ / „Auftragsverarbeiter“)

Und

(nachfolgend „Auftraggeber“ / „Verantwortlicher“)

Präambel

Diese Vereinbarung zur Auftragsverarbeitung (nachfolgend „AV“) regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Hinblick auf die Erfüllung und Einhaltung gesetzlicher Bestimmungen zum Datenschutz. Die gesetzlichen Grundlagen bilden die Regelungen der Europäischen Datenschutzgrundverordnung (nachfolgend „DS-GVO“) und des Bundesdatenschutzgesetzes (nachfolgend „BDSG“, n.F. vom 25. Mai 2018).

Begriffsbestimmungen

„Auftragsverarbeiter“ bezeichnet diejenige natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„Betroffener“ bezeichnet die identifizierte oder identifizierbare natürliche Person, auf die sich personenbezogene Daten beziehen.

„Personenbezogene Daten“ sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person.

„Subunternehmer“ bezeichnet sämtliche von Seiten des Auftragsverarbeiters beauftragte weitere Auftragsverarbeiter (Unterauftragsverhältnis), um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen.

„Verantwortlicher“ bezeichnet diejenige natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

„Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ist die im Folgenden beschriebene Leistungserbringung durch den Auftragsverarbeiter.

Gegenstand des Auftrags ist die Erbringung von IT- Dienstleistungen im Bereich des Supports/Administration von Server-Systemen für den Verantwortlichen.

(2) Die Dauer des Auftrags ergibt sich aus der Leistungsvereinbarung.

Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 2 Umfang und Art der vorgesehenen Verarbeitung von Daten

(1) Gegenstand des Auftrags ist nicht die originäre Nutzung oder Verarbeitung personenbezogener Daten des Verantwortlichen durch den Auftragsverarbeiter. Im Rahmen der Leistungserbringung durch den Auftragsverarbeiter kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden. Die Art der personenbezogenen Daten und Kreis der Betroffenen hängt davon ab, welche Daten sich auf dem Server- System befinden, auf dem die IT-Dienstleistung erbracht wird.

(2) Im Rahmen der Leistungserbringung werden die folgenden Daten von betroffenen Personengruppen Bestandteil der Datenverarbeitung. Dies richtet sich danach, welche Daten auf den Datenverarbeitungssystemen liegen, auf denen der Auftragnehmer den Dienstleistungsauftrag ausführt.

Kreis der Betroffenen

- | | |
|--|---|
| <input type="checkbox"/> Mitarbeiter, Bewerber, Praktikanten, Azubis | <input type="checkbox"/> Kunden / Interessenten |
| <input type="checkbox"/> Patienten, Angehörige | <input type="checkbox"/> Mitglieder (z.B. von Vereinen) |
| <input type="checkbox"/> Lieferanten / Dienstleister | <input type="checkbox"/> Webseitenbesucher |
| <input type="checkbox"/> Sponsoren | <input type="checkbox"/> Makler, Vermittler |
| <input type="checkbox"/> Mieter | <input type="checkbox"/> Abonnenten |
| <input type="checkbox"/> Handelsvertreter | <input type="checkbox"/> Sonstige: _____ |

Art der personenbezogenen Daten

- | | |
|---|--|
| <input type="checkbox"/> Name, Vorname, Anrede | <input type="checkbox"/> Geburtsdaten |
| <input type="checkbox"/> Informationen zum Familienstand | <input type="checkbox"/> Kontaktdaten |
| <input type="checkbox"/> Vertragsdaten | <input type="checkbox"/> Bank-, Finanz-, Konto-, Transaktionsdaten |
| <input type="checkbox"/> Abrechnungsdaten | <input type="checkbox"/> Leistungsdaten |
| <input type="checkbox"/> Gesundheitsdaten | <input type="checkbox"/> Mitarbeiter- / Personaldaten |
| <input type="checkbox"/> Ortungsdaten | <input type="checkbox"/> Biometrische, genetische Daten |
| <input type="checkbox"/> Videoaufzeichnungen | <input type="checkbox"/> Bilddateien, Fotos |
| <input type="checkbox"/> Protokolldateien mit Personenbezug | <input type="checkbox"/> IP-Adresse |
| <input type="checkbox"/> Auswertungen | <input type="checkbox"/> Geodaten / Geoinformationen |
| <input type="checkbox"/> Auskünfte (z.B. von Auskunftsteien) | <input type="checkbox"/> Besondere Arten personenbezogener Daten |
| <input type="checkbox"/> Rassistische oder ethnische Herkunft | <input type="checkbox"/> Religionszugehörigkeit |

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Datenschutzauditoren, Qualitätsauditoren)

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer eine angemessene Vergütung geltend machen.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Auftrages und der Weisung des Auftraggebers. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen unverzüglich nach Kenntnisnahme mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen sowie bei der Einhaltung und Durchführung von Melde- und Informationspflichten gemäß DS-GVO.

Des Weiteren unterstützt der Auftragnehmer den Auftraggeber bei der Erstellung von Verzeichnissen von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO und teilt ihm die jeweils erforderlichen Angaben in geeigneter Weise mit.

(3) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Der Auftragnehmer gewährleistet ferner, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung bis zur Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

(5) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen oder die erteilten Weisungen des Auftraggebers, der im Rahmen der Verarbeitung durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen.

Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DS-GVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

Stellt der Auftragnehmer fest oder begründen Tatsachen die Annahme, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, unterrichtet er den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalles in Schriftform. Die Information hat eine Darlegung der Art der unrechtmäßigen Kenntniserlangung sowie mögliche nachteilige Folgen der unrechtmäßigen Kenntniserlangung zu beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung oder Kenntnisnahme durch Dritte künftig zu verhindern.

(6) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 DS-GVO bestellt hat.

Als Datenschutzbeauftragter für den Auftragnehmer ist bestellt
Herr Sven Brodermanns, EU-CON BeraterForum GmbH, E-Mail: brodermanns@eu-con.net, Telefon:
02452 993311, Mobil: 0162 2328919.

§ 6 Technisch-organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer hat die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten und ihre Einhaltung zu überwachen. Er versichert, dass er die gesetzlichen Bestimmungen zur Sicherheit bei der Auftragsverarbeitung gemäß Art. 28 Abs 3 c i.V.m. Art. 32 DS-GVO einhält. Hierzu hat er angemessene Maßnahmen der Datensicherheit (technisch-organisatorische Maßnahmen; TOM) getroffen und gewährleistet unter fortlaufender Vornahme gegebenenfalls erforderlicher Anpassungen ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Datenverarbeitungssysteme. Hierbei wird dem Stand der Technik, der Verhältnismäßigkeit und die Art, der Umfang und die Zwecke der Datenverarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen Rechnung getragen.

(2) Der Auftragnehmer hat die technisch-organisatorischen Maßnahmen vor Beginn der Datenverarbeitung zu dokumentieren und stellt sie dem Auftraggeber im Anhang dieser Vereinbarung zur Prüfung zur Verfügung. Mit Abschluss dieser Vereinbarung werden die dokumentierten Maßnahmen Grundlage der Auftragsverarbeitung.

(3) Die technisch-organisatorischen Maßnahmen unterliegen dem technischen Fortschritt. Dem Auftragnehmer ist es insoweit gestattet, alternative adäquate Maßnahmen umzusetzen. Das Sicherheitsniveau der in dieser Vereinbarung festgelegten Maßnahmen darf dabei jedoch nicht unterschritten werden.

§ 7 Unterauftragsverhältnisse

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen und, soweit für die Geschäftsabwicklung notwendig, Subunternehmer mit Leistungen unterbeauftragt. In der Anlage 1 sind die zu diesem Zeitpunkt eingesetzten Subunternehmer aufgeführt, die je nach Aufgabenstellung des Auftraggebers zum Einsatz kommen können.

Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Auftrag dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Auftrages.

(2) Ein Unterauftragsverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistungserbringung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutzmaßnahmen zu gewährleisten.

Nicht zu den Unterauftragsverhältnissen gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsdienstleistungen, Post- oder Transportdienstleistungen, Wartung oder Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und rechtskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Erbringt ein Unterauftragnehmer die vereinbarte Leistung nicht innerhalb eines Mitgliedsstaates der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt auch, wenn Dienstleister lediglich zur Erbringung von Nebenleistungen i.S.d. Abs. 2 eingesetzt werden sollen.

Der Auftraggeber kann der Änderung innerhalb einer angemessenen Frist aus wichtigem Grund gegenüber dem Auftragnehmer widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung oder Ergänzung als gegeben.

§ 8 Beendigung und Rückgabe von Daten, Zurückbehaltungsrecht

(1) 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 Grundlage einer Einzelbeauftragung durch den Auftraggeber oder gibt die Daten an den Auftraggeber zurück.

(2) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

(3) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (z.B. durch Pfändung oder Beschlagnahme), durch Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der

Auftragnehmer wird die Gläubiger über die Tatsache unverzüglich informieren, dass es sich um Daten handelt, die im Auftrag verarbeitet werden.

(2) Es gilt deutsches Recht. Als Gerichtsstand wird der Sitz des Auftragnehmers vereinbart.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen einer schriftlichen Vereinbarung.

(4) Bei etwaigen Widersprüchen zum Hauptvertrag gehen die in diesem Auftragsverarbeitungsvertrag getroffenen Regelungen vor. Sollten einzelne Teile dieser Regelung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen nicht.

Ort, Datum

Ort, Datum

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Anlagen
Technisch-organisatorische Maßnahmen
Anlage 1 Subunternehmer

Anlage 1

Einsatz eines Subunternehmers

Untenstehender Subunternehmer sind vom Auftragnehmer beauftragt:

Name und Anschrift des Unterauftragnehmers	Beschreibung der Leistung des Unterauftragnehmers
COYOOT GmbH, Nelkenstr. 19, 67691 Hochspeyer, Herr Germann	JobRouter Consultant
Alfa systems, Alfred Faltermeier, Hopfenstr. 22, 63454 Hanau	Softwarehaus
Schwass Unternehmensberatung, Rotdornstr. 6, 22880 Wedel	Unternehmensberatung
Gerhard Thress, Jahnstraße 5, 63179 Obertshausen	Softwarehaus
Kabema Consulting GmbH, Bucher Chaussee 5, 13125 Berlin	Consultant
JobRouter AG, Besselstrasse 26, 68219 Mannheim	Softwarehaus

Zudem ist es möglich, dass die Hersteller der Anwendungen ELO oder JobRouter im Rahmen des Third-Level-Wartungsvertrages für den Auftraggeber tätig werden.

Allgemeine technische und organisatorische Maßnahmen Art. 32 DS-GVO

1. Allgemeine Angaben	Gültig für KaiTech IT-Systems GmbH, Im Dörener Feld 2, 33100 Paderborn Stand: 31.03.2018
2. Vertraulichkeit	
2.1 Zutrittskontrolle	<p>Alarmanlage mit Bewegungs- und Rauchmeldern, verbunden mit einem Wachschutzunternehmen.</p> <p>Der Gebäudezutritt erfolgt über Schlüssel und Chipkarte.</p> <p>Die Schlüssel- Chipvergabe ist protokolliert</p> <p>Nur führenden Mitarbeitern wird ein Schlüssel ausgehändigt.</p> <p>Der Zutritt zu den Büroräumen erfolgt nach Anmeldung beim Empfang.</p> <p>Der Serverraum, in dem sich sämtliche DV-Anlagen befinden, ist im hinteren Bereich des Gebäudes untergebracht.</p> <p>Ein unbemerkter Zutritt durch Dritte kann ausgeschlossen werden, da die Eingangstür ständig verschlossen ist und nur nach Kontrolle geöffnet wird.</p>
2.2 Zugangskontrolle	Eine unbefugte Nutzung der DV-Systeme kann zum jetzigen Zeitpunkt ausgeschlossen werden. Der Großteil der Mitarbeiter ist IT-technisch versiert und kennt sich mit dem Schutz der DV-Anlagen aus, und setzt dies auch im Sinne der Geschäftsleitung im Alltag um. Weiterhin ist die Bedeutung der IT für das Unternehmen diesem Personenkreis hinlänglich bekannt.
2.3 Zugriffskontrolle	<p>Für den Zugriff auf die gespeicherten Daten sind eindeutige Regeln definiert.</p> <p>Grundsätzlich sind Zugriffe auf bestimmte Programme und Daten nur mit speziellen Passwörtern möglich.</p> <p>Die Daten der Firma KaiTech werden durch permanente Back-Ups geschützt (Großvater-Vater-Sohn Prinzip). Das System generiert automatisch Warnungen, sollte innerhalb der Sicherungen etwas nicht in Ordnung sein.</p>
3. Integrität	
3.1. Weitergabekontrolle	<p>Eine Weitergabe der personenbezogenen Daten des Auftraggebers an KaiTech ist nicht vorgesehen und bedarf der ausdrücklichen Weisung des Auftraggebers. Der Auftraggeber hat die Weitergabe zu kontrollieren und zu protokollieren.</p> <p>Die Weitergabe der Daten erfolgt über den verschlüsselten Zugang über TeamViewer.</p>

3.2 Eingabekontrolle	Sämtliche Datenverarbeitung darf ausschließlich gemäß den Weisungen des Auftraggebers und den vertraglichen Vereinbarungen erfolgen (auftragsbezogen).
4. Verfügbarkeitskontrolle	<p>Personenbezogene Daten vom Auftraggeber werden nur zu Testzwecken, Problemlösungen oder Entwicklungen beim Auftragnehmer vorgehalten und nach Auftragsabarbeitung gelöscht. Sollten Daten für die Auftragsbearbeitung beim Auftragnehmer vorgehalten werden, erfolgt die Speicherung auf verschlüsselten externen Datenträgern. Backups werden bezüglich der personenbezogenen Daten des Auftraggebers nicht erstellt. Der Auftragnehmer gewährleistet nicht die Verfügbarkeit personenbezogener Daten des Auftraggebers. Die lokalen IT-Komponenten beim Auftragnehmer (Server und Netzwerkinfrastruktur) sind durch eine unterbrechungsfreie Stromversorgung auszustatten, die einen Stromausfall von 10 Minuten überbrückt. Gegen Ende der Notlaufzeit ist die DVA sicher herunterzufahren.</p> <p>Folgende Schutzmaßnahmen sind eingerichtet:</p> <ul style="list-style-type: none"> - Firewall - Virenschutzprogramm - Recovery Pläne zur Wiederherstellung der Datensicherung