xentral Customer Care
Vertrag über die Auftragsverarbeitung von personenbezogenen Daten

Stand 11.10.2019

zwischen

_____
__

_____
__

_____
__
(Firma, Adresse, Tel/Fax/Mail)

- nachstehend „Auftraggeber“ genannt -

und

Xentral ERP Software GmbH, Fuggerstrasse 11, 86150 Augsburg

- nachfolgend „Auftragnehmer“ genannt -

- beide zusammen nachfolgend „Parteien“ genannt -

Präambel 2

§ 1 Gegenstand und Dauer der Datenverarbeitung 2

§ 2 Umfang, Art und Zweck der Datenverarbeitung und Betroffene 2

§ 3 Verantwortung, einschließlich Weisungen 3

§ 4 Kontrollen 4

§ 5 Grundsätze der technisch-organisatorische Maßnahmen 5

§ 6 Einschaltung von Subunternehmern 5

§ 7 Berichtigung, Löschung und Sperrung von Daten 6

§ 8 Haftung, Freistellung und Vertragsstrafen 6

§ 9 Sonstige Bestimmungen 7

Präambel

(1) Der Auftragnehmer erhebt, verarbeitet und nutzt personenbezogene Daten des Auftraggebers im Rahmen der Durchführung einzelner Pflegeleistungen an der Software Xentral und evtl. damit verbundener EDV-Systeme. Zu diesem Zweck haben die Parteien bereits ein Angebot verständigt über SaaS und/oder die Erbringung von Pflege (Xentral Customer Care – Allgemeine Geschäftsbedingungen) geschlossen (nachfolgend „Customer Care–AGB“).

(2) Bei der Erbringung dieser Leistungen werden ebenfalls personenbezogene Daten des Auftraggebers durch den Auftragnehmer erhoben, verarbeitet und genutzt (nachfolgend „Datenverarbeitung“).

(3) Die Parteien wollen ihren wechselseitigen datenschutzrechtlichen Verpflichtungen nach Art. 28, 4 Nr. 2 Datenschutzgrundverordnung (EU) 2016/679 (nachfolgend „DSGVO“) Rechnung tragen und schließen deswegen nachstehenden Vertrag über die zur Auftragsdatenverarbeitung (nachfolgend „AV-Vertrag“) der sich in einzelnen Punkten auf die Customer Care-AGB bezieht.

§ 1 Gegenstand und Dauer der Datenverarbeitung

(1) Gegenstand der Datenverarbeitung

(a) Inhaltlicher Geltungsbereich

Gegenstand dieses AV-Vertrags ist die Erbringung der im Angebot beschriebenen Software as a Service (SaaS) und /oder Pflegeleistungen für die Software „Xentral“ für den Auftraggeber.

Dieser AV-Vertrag gilt für sämtliche Tätigkeiten bei denen Mitarbeiter und/oder - soweit gem. nachstehendem § 6 zulässig - Subunternehmer des Auftragnehmers personenbezogene Daten des Auftraggebers erheben, verarbeiten oder nutzen.

(b) Räumlicher Geltungsbereich

Nach diesem AV-Vertrag ist die Datenverarbeitung weltweit zulässig, d.h. im Gebiet des

Gebietes der Europäischen Union und des Europäischen Wirtschaftsraumes (EWG) und sichere Drittstaaten (Art. 45 DSGVO) und weiterer Staaten gemäß Art. 46 DSGVO.

(2) Dauer der Datenverarbeitung

Dieser AV-Vertrag tritt mit Unterzeichnung durch beide Parteien in Kraft. Der AV-Vertrag kann mit einer Frist von 3 Monaten zum Monatsende ordentlich durch eine der Parteien gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt davon unberührt.

§ 2 Umfang, Art und Zweck der Datenverarbeitung und Betroffene

(1) Umfang und Zweck der Datenverarbeitung

Im Rahmen der Bestellung des Auftraggebers gemäß 2.1 Customer Care-AGB gestaltet sich Umfang und Zweck der Datenverarbeitung

- SaaS-Betrieb gemäß Angebot
- Betrieb eines Ticket-System (Ziffer 2.5 Customer Care-AGB) und/oder
- Notfall-Hotfix/-Telefon (Ziffer 3 Customer Care-AGB) und/oder
- Hotline-Service (Ziffer 4 Customer Care-AGB) und/oder
- Installationsunterstützung (Ziffer 5.2 Customer Care-AGB).

Der von Auftraggeber dafür zu vergütende Aufwand ergibt sich aus Anhang 2, soweit er nicht bereits im Rahmen der Customer Care-AGB den bestellten Leistungen des Kunden abgegolten ist.

(2) Art der Daten der Datenverarbeitung

Im Rahmen des AV-Vertrags erhebt, verarbeitet und nutzt der Auftragnehmer folgende Arten von Daten und hat hierauf die Möglichkeit eines Zugriffs:

- Personenstammdaten
- Kommunikationsdaten (zB Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkte- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, zB Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Weitere/Abweichende Datenarten gemäß Anhang 3 (soweit vorhanden, vom Auftraggeber beizufügen)

(3) Kreis der Betroffenen

Der Kreis der durch den Umgang mit personenbezogenen Daten im Rahmen dieses AV-Vertrags Betroffenen umfasst:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Weitere/Abweichende Betroffene gemäß Anhang 4 (soweit vorhanden, vom Auftraggeber beizufügen)

§ 3 Verantwortung, einschließlich Weisungen

3.1 Verantwortung des Auftraggebers

(1) Der Auftraggeber ist im Hinblick auf die Datenverarbeitung für die Einhaltung sämtlicher einschlägiger Datenschutz- vorschriften, insb. der DSGVO und des Bundesdatenschutzgesetzes („BDSG“ in der Fassung ab 25.5.2018), verantwortlich soweit darin keine Aufgaben explizit dem Auftragnehmer zugewiesen sind (vgl. Art. 28 DSGVO)

Der Auftraggeber ist insb. dafür verantwortlich, dass

- er die Zulässigkeit der Verarbeitung gem. Art. 6 Abs. 1 DSGVO beurteilt, insbes. etwaige Einwilligungserklärungen und/oder Betriebsvereinbarungen die für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten erforderlich sind, eingeholt wurden und die gesetzlichen Erlaubnistatbestände dazu vorliegen.
- die Rechte der Betroffenen (Art. 12 – 23 DSGVO) gewährt werden.
- der Auftragnehmer bei der Durchführung der Pflegeleistungen nach diesem AV-Vertrag mit möglichst wenig personenbezogenen Daten in Kontakt kommt gemäß Art. 25 DSGVO.
- er angemessene Vorkehrungen für den Fall trifft, dass Xentral ganz oder teilweise nicht ordnungsgemäß arbeitet (z.B. durch tägliche Datensicherung, Störungsdiagnose, regelmäßige Überprüfung der Daten- verarbeitungsergebnisse).
- er den Auftragnehmer vor einem Datenzugriff im Wege der Fernwartung rechtzeitig vorab darauf hinzuweist, inwieweit seine Daten nicht gegen Datenverlust gesichert sind. Ohne einen solchen Hinweis darf der Auftragnehmer davon ausgehen, dass alle Daten des Auftraggebers gegen Datenverlust gesichert sind, auf die der Auftragnehmer Zugriff erhält.

(2) Der Auftraggeber ist „Verantwortlicher“ und „Herr der Daten“, vgl. Art. 4 Abs. 7 DSGVO. Der Auftragnehmer verarbeitet die Daten ausschließlich zur Durchführung nach Weisung des Auftraggebers gemäß diesem AV-Vertrag. Darüber hinaus gilt:

- Sämtliche Weisungen des Auftraggebers zum Zeitpunkt des Abschlusses dieses AV-Vertrags finden sich abschließend in den Regelungen dieses AV-Vertrags und seinen Anhängen. Weitere Weisungen erteilt der Auftraggeber nur soweit diese zur Durchführung der Datenverarbeitung erforderlich sind. Der Auftraggeber erteilt seine Weisungen nur in Schrift- oder Textform und in dokumentierter Art und Weise.
- Der Auftraggeber wird gegenüber dem Auftragnehmer weisungsberechtigte Personen und Ihre Vertreter wenigstens in Textform benennen. Ohne Benennung gelten nur die Support-berechtigten Personen (9.2 Customer Care-AGB) als weisungsberechtigt im Sinne dieses AV-Vertrags.

(3) Der Auftraggeber ist verpflichtet, den Aufwand des Auftragnehmers gemäß der aktuellen Preisliste (Anhang 2) zu vergüten, soweit dem Auftragnehmer durch

- die Befolgung oder Ausgestaltung einer Weisung;
- die Unterstützung bei der Erfüllung der Rechte eines Betroffenen (Art. 12 – 23 DSGVO) oder
- Unterstützung bei der Erfüllung von Art. 32 – 36 DSGVO sowie der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Aufwand entsteht. Die Vergütungspflicht für den Aufwand des Auftragnehmers bei der

Unterstützung des Auftraggebers zur Erfüllung der Informationspflichten aus Art. 33 DSGVO ergibt sich aus dem folgenden § 3.2 (4) Satz 2.

(4) Der Auftraggeber weist den Auftragnehmer daraufhin, wenn und soweit die technischen und organisatorischen Maßnahmen (Anhang 1) und/oder die übrigen Vorgaben dieses AV-Vertrags nicht mehr den gültigen Datenschutzvorschriften entsprechen, die auf den Auftraggeber Anwendung finden (inkl. gesetzlicher Neuerungen). Der Auftraggeber ist verpflichtet, den Aufwand des Auftragnehmers für die Anpassung des AV-Vertrags und/ oder der vorgenannten Maßnahmen gemäß der aktuellen Preisliste (Anhang 2) zu vergüten, soweit dem Auftragnehmer Aufwand durch die Umsetzung neuer, vom Auftraggeber geforderter technischer oder organisatorischer Maßnahmen entstehen.

Der Auftraggeber ist sich insbesondere im Klaren darüber, dass der Auftragnehmer grundsätzlich nur eine unverschlüsselte Kommunikation per E-Mail anbietet und dass durch einen unverschlüsselten E-Mail-Verkehr keine ausreichende Geheimhaltung gegenüber Dritten gewährleistet werden kann. Wünscht der Auftraggeber eine Verschlüsselung der E-Mail-Kommunikation wird er hierzu das Ticket-System (gemäß 2.5 Customer Care-AGB) verwenden und/oder sich mit dem Auftragnehmer abstimmen.

(5) Der Auftraggeber informiert den Auftragnehmer über jeden aktuellen Informationsaustausch mit den Datenschutzbehörden mit dem Auftraggeber, soweit dieser Austausch die Datenverarbeitung nach diesem AV-Vertrag betrifft oder betreffen könnte.

3.2 Verantwortung des Auftragnehmers

(1) Der Auftragnehmer wird personenbezogene Daten, die er im Rahmen dieses AV-Vertrags im Auftrag für den Auftraggeber verarbeitet, ausschließlich zur Erfüllung dieses AV-Vertrags verarbeiten sofern er nicht zu einer anderen Verarbeitung durch EU-Recht oder dem anwendbaren Recht eines Mitgliedsstaates verpflichtet ist (z.B. Ermittlungen von Strafverfolgungsbehörden); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Wenn und soweit der Auftragnehmer der Auffassung ist, dass die Ausführung von Weisungen des Auftraggebers iS des vorstehenden Absatzes zu einer Verletzung von Datenschutzbestimmungen führt, ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich hierauf hinzuweisen (Art. 28 Abs. 3 S. 3 DSGVO). In diesem Fall ist er berechtigt, die Durchführung der entsprechenden Weisung des Auftraggebers so lange auszusetzen, bis sie durch den Ansprechpartner des Auftraggebers bestätigt oder geändert wird.

(3) Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich zu informieren, wenn und soweit er oder die bei ihm beschäftigten Personen gegen Datenschutz- oder gegen Bestimmungen dieses AV-Vertrags verstoßen haben.

(4) Der Auftragnehmer wird den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 30, 32 - 36 DSGVO angemessen unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der

Verarbeitung personenbezogener Daten mit. Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen. Der Auftraggeber ist verpflichtet, den Auftragnehmer den durch diese Unterstützung entstehenden Aufwand gemäß der aktuellen Preisliste (Anhang 2) zu vergüten, soweit der Auftragnehmer die Informationspflicht des Auftraggebers nicht schuldhaft verursacht hat.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei Erfüllung Rechten der Betroffenen (Art. 12 – 23 DSGVO), wenn der Auftraggeber hierzu eine dokumentierte Aufforderung (schriftlich oder in Textform) an den Auftragnehmer abgegeben hat. Die Vergütungspflicht ergibt sich aus § 3.1 (3).

§ 4 Kontrollen

(1) Der Auftragnehmer wird seine, zur Datenverarbeitung befugten Mitarbeiter auf zur Vertraulichkeit verpflichten und dies kontrollieren. Der Auftragnehmer weist dem Auftraggeber diese Verpflichtung auf das Datengeheimnis auf Anfrage nach.

(2) Der Auftragnehmer ist berechtigt, den Nachweis über die Einhaltung des Datenschutzes und der Datensicherheit, insbes. Nach Art. 28 (3) lit. h. DSGVO bei sich und/oder Subunternehmern durch die Vorlage von Testate zu erbringen. Eine Kontrolle vor Ort entfällt dadurch, sofern keine außergewöhnlichen Anlässe bestehen (§ 4 (3) Abs. 2). Die Testate sind vom Auftragnehmer max. einmal jährlich zu aktualisieren.

(3) Falls der Auftragnehmer nach § 4 (2) keine aktuellen Testate vorlegen kann, kann der Auftraggeber die Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit beim Auftragnehmer zu dessen üblichen Geschäftszeiten einmal jährlich stichprobenartig zu kontrollieren, soweit keine Anhaltspunkte für einen Verstoß des Auftragnehmers gegen die Weisungen des Auftraggebers oder gegen diesen AV-Vertrag vorliegen.

Im Übrigen kann der Auftraggeber die vorgenannten Kontrollen jederzeit durchführen, wenn bestimmte Anhaltspunkte für einen Verstoß des Auftragnehmers gegen die Weisungen des Auftraggebers bestehen oder dafür, dass der Auftraggeber gegen diesen AV-Vertrag verstoßen hat.

(4) Die Kontrollen nach § 4 (2) und (3) AV-Vertrag werden vom Auftraggeber mindestens 21 Tage im Voraus angekündigt und hinsichtlich des Gegenstands und des Umfangs mit dem Auftragnehmer abgestimmt.

(5) Zur Ausführung der Kontrollen nach § 4 (3) AV-Vertrag wird der Auftragnehmer dem Auftraggeber insbesondere Zugang zu den Datenverarbeitungsanlagen gewähren, die für die Datenverarbeitung nach diesem AV-Vertrag bestimmt sind.

(6) Zur Kontrolle nach § 4 (3) AV-Vertrag seitens des Auftraggebers sind – soweit vorhanden - dessen Datenschutzbeauftragter oder vom Auftraggeber bestellte neutrale IT-Sachverständige befugt, soweit diese strafbewehrt erklären, die berechtigten Geheimhaltungs- und Datenschutzinteressen des Auftragnehmers und dessen weitere Kunden zu wahren.

(7) Der Auftragnehmer ist verpflichtet, der für den Auftraggeber zuständigen Datenschutzbehörde im gesetzliche erforderlichen Umfang Zugang zu seinen Geschäftsräumen und Aufzeichnungen über die Datenverarbeitung für den Auftraggeber zu gewähren. Für den Fall, dass behördliche Kontrollen durch den Auftraggeber veranlasst sind, wird dieser

dem Auftragnehmer den, durch die Kontrollen entstehenden Aufwand gemäß Anhang 2 ersetzen.

§ 5 Grundsätze der technisch-organisatorische Maßnahmen

(1) Die technischen und organisatorischen Maßnahmen gemäß § 32 DSGVO werden in Abstimmung mit dem Auftraggeber ergriffen (Anhang 1).

(2) Diese Maßnahmen (Anhang 1) unterliegen dem technischen Fortschritt und dürfen vom Auftragnehmer durch andere adäquate Maßnahmen ersetzt werden, soweit damit das ursprüngliche Sicherheitsniveau nicht unterschritten wird. Der Auftragnehmer wird solche Ersetzungen dokumentieren und dem Auftraggeber auf schriftliche Anfrage zur Verfügung stellen.

(3) Der Datenschutzbeauftragte des Auftragnehmers ist in Anlage 1 hinterlegt. Er kann einseitig durch den Auftragnehmer geändert werden. Sollten sich dadurch die Kontaktdaten des Datenschutzbeauftragten ändern, wird der Auftragnehmer dies dem Auftraggeber mitteilen.

§ 6 Einschaltung von Subunternehmern

(1) Allgemeine Genehmigung für die Einschaltung von Subunternehmern

Der Auftragnehmer ist unbeschadet § 6 (2) (b) allgemein berechtigt, in seinem Ermessen Subunternehmern zur Leistungserbringung für diesen AV-Vertrag einzuschalten, soweit diese über geeignete technische und organisatorische Maßnahmen verfügt, sowie den Anforderungen von Art. 28 Abs. 4 S. 1, Abs. 3 DSGVO genügt.

(2) Anforderungen an die Einschaltung von Subunternehmern

Wenn und soweit der Auftragnehmer nach Maßgabe des vorstehenden § 6 (1) Subunternehmer einschaltet, sind die vertraglichen Vereinbarungen mit diesen so zu gestalten, dass sie den Anforderungen an den Datenschutz und die Datensicherheit, wie sie im Verhältnis zwischen den Parteien bestehen, entsprechen.

(a) Hierbei stellt der Auftragnehmer insb. sicher, dass die in diesem AV-Vertrag festgelegten Regelungen auch im Verhältnis zu den Subunternehmern gelten; soweit der Auftraggeber nicht der Zuziehung bestimmter Subunternehmer im Einzelfall zugestimmt hat. Diese Zustimmung gilt als erteilt, wenn (i) für die in Anhang 5 niedergelegten Subunternehmer oder wenn (ii) der Auftragnehmer dem Auftraggeber die Einschaltung eines Subunternehmers unter abweichenden Regelungen angezeigt hat und der Auftraggeber dem nicht innerhalb von 6 Wochen wenigstens in Textform widersprochen hat. In jedem Fall wird dem Auftraggeber auf dessen Verlangen hin Auskunft über die entsprechenden vertraglichen Regelungen mit dem Subunternehmer geben und ihm auf Verlangen die entsprechenden Vertragsunterlagen vorlegen.

(b) Der Auftragsverarbeiter informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 S. 2 DSGVO).

(3) Kontrollrechte des Auftraggebers

Bei seinen vertraglichen Vereinbarungen mit Subunternehmern stellt der Auftragnehmer sicher, dass der Auftraggeber berechtigt ist, bei den Subunternehmern Kontrollen vor Ort durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der

Auftragnehmer stellt namentlich sicher, dass dem Auftraggeber die Überprüfungsrechte nach Art. 28 Abs. 3 h) DSGVO eingeräumt werden.

§ 7 Berichtigung, Löschung und Sperrung von Daten

(1) Die im Auftrag des Auftraggebers erhobenen, verarbeiteten und genutzten Daten wird der Auftragnehmer nur nach Weisung des Auftraggebers berichtigen, löschen oder sperren, wenn berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Wenn sich ein Betroffener zu diesem Zweck direkt an den Auftragnehmer wendet, hat dieser ein solches Ersuchen unverzüglich an den Auftraggeber weiterzuleiten.

(2) Der Ansprechpartner des Auftraggebers wird das Ersuchen nach § 7 (1) S. 2 unverzüglich prüfen und dem Auftragnehmer schriftlich mitteilen, ob es berechtigt war oder nicht und den Auftragnehmer anweisen, die Berichtigung, Löschung oder Sperrung vorzunehmen.

(3) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder wie in Anhang 1 beschrieben zu löschen. Der Auftraggeber hat die Entscheidung hierüber spätestens bei der Kündigungserklärung - oder im Fall von Laufzeitverträgen min. 6 Wochen vor Laufzeitende – in Textform anzuzeigen.

§ 8 Haftung, Freistellung und Vertragsstrafen

(1) Haftung des Auftragnehmers

Der Auftraggeber haftet sinngemäß im Rahmen von § 8 (2) gegenüber dem Auftragnehmer, soweit der Auftraggeber schuldhaft gegen anwendbare Datenschutzvorschriften verstoßen hat für die der Auftragnehmer in Anspruch genommen wurde. Die Einhaltung von Datenschutzverstößen nach § 3 (1) S. 2, (2) – (5) gilt hierbei als Kardinalspflicht.

(2) Haftung des Auftragnehmers gegenüber dem Auftraggeber

(1) In folgenden Fällen haftet der Auftragnehmer auf Grundlage vertraglicher und außervertraglicher Pflichtverletzungen für Schadensersatz oder Ersatz vergeblicher Aufwendungen in unbeschränkter Höhe und nach den gesetzlichen Verjährungsfristen:

a. bei Vorsatz seitens des Auftragnehmers,

b. bei arglistigem Verschweigen eines Mangels seitens des Auftragnehmer,

c. bei von Auftragnehmer zu verantwortenden Personenschäden,

d. bei Garantien von Auftragnehmer und

e. bei Ansprüchen nach dem Produkt- haftungsgesetz gegen den Auftragnehmer

(2) In den Fällen grober Fahrlässigkeit haftet der Auftragnehmer nur für den vorhersehbaren Schaden, der durch die verletzte Pflicht verhindert werden sollte.

(3) Die Haftung gemäß § 8 (2) (2) ist beschränkt auf 100.000,00 EUR pro Schadensfall und insgesamt für alle Schadensfälle aus dem Vertragsverhältnis auf 250.000,00 EUR.

(4) In den Fällen einfacher Fahrlässigkeit haftet der Auftragnehmer bei einer Verletzung vertragswesentlicher Pflichten für den vorhersehbaren Schaden, der durch die verletzte Pflicht verhindert werden sollte. Eine vertragswesentliche Pflicht ist eine Pflicht, deren

Erfüllung die ordnungsgemäße Durchführung dieses Vertrages erst ermöglicht oder deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf.

(5) Die Haftung gemäß Ziffer § 8 (2) (4) ist beschränkt auf 100.000,00 EUR pro Schadensfall, insgesamt für alle Schadensfälle aus dem Vertragsverhältnis auf 250.000,00 EUR.

(6) Unbeschadet der Ziffern 1(1) - (5) ist die Haftung des Auftragnehmers ausgeschlossen, d.h. insbesondere für höhere Gewalt (inkl. Streiks, Naturkatastrophen) und für die einfache fahrlässige Verletzung nicht-vertragswesentlicher Pflichten.

(7) Die Verjährungsfrist der Ansprüche aus Ziffer § 8 (2) (4) beträgt ein Jahr. Sie beginnt mit dem in § 199 Abs. 1 BGB bestimmten Zeitpunkt.

(8) Dem Auftragnehmer bleibt der Einwand des Mitverschuldens (z.B. wegen Verletzungen der Pflichten des Auftraggebers nach § 3) unbenommen. Kommt der Auftraggeber insbesondere seiner Obliegenheit zur regelmäßigen Datensicherung (§ 3 (1) Bulletpoint 4 und 5) nicht oder nicht vollständig nach und entsteht ihm ein Schaden, der ganz oder zum Teil nicht eingetreten wäre, wenn der Auftraggeber eine solche Datensicherung durchgeführt hätte, so hat der Auftraggeber sich die mangelnde Datensicherung bei der Berechnung des Umfanges des Schadensersatzes in Form eines angemessenen Mitverschuldensanteils anzurechnen.

§ 9 Sonstige Bestimmungen

(1) Bei Widersprüchen zwischen diesem AV-Vertrag seinen Anhängen gehen die Regelungen dieses AV-Vertrags vor.

(2) Der Gerichtsstand und Leistungsort für diesen AV-Vertrag ist Augsburg.

(3) Sollten einzelne Bestimmungen dieses AV-Vertrags unwirksam oder lückenhaft sein, so bleiben die übrigen Bestimmungen wirksam. Sollten zur Ausfüllung lückenhafter oder unwirksamer Bestimmungen mehrere gesetzliche Bestimmungen alternativ zur Anwendung kommen können, so gilt jene gesetzliche Bestimmung, die dem wirtschaftlichen Willen der Parteien am nächsten kommt.

Anhänge:

1 - Technisch-organisatorische Maßnahmen
2 – Vergütungsbedingungen und Preisliste
3 – Abweichende Datenarten (soweit vorhanden)
4 – Abweichende Betroffene (soweit vorhanden)
5 – Subunternehmer

_____

Ort, Datum, Unterschrift Auftraggeber

_____

Ort, Datum, Unterschrift Auftragnehmer

Anhang 1 - Technisch-organisatorische Maßnahmen

Datenschutzbeauftragter des Auftragnehmers:

Maximilian Hartung

c/o Xentral ERP Software GmbH

Fuggerstrasse 11

86150 Augsburg

Tel. +821 268 41 0 41

Fax. +821 268 41 0 42

kontakt@xentral.biz

A. Pseudonymisierungs- und Verschlüsselungsmaßnahmen

Siehe Ziff.

- B.2 Punkt 3
- B.4. Punkte 3 und 4
- B.7. Punkt 3

B. Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer

1. Zutrittskontrolle, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet und genutzt werden, verwehrt:
   - Die Geschäftsräume des Auftragnehmers werden nach Dienstschluss abgesperrt.
   - Es existiert eine protokollierte Schlüsselvergabe der Schlüssel für die Geschäftsräume des Kunden.
2. Zugangskontrolle, die es verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:
   - Der Auftragnehmer unterhält schriftliche Regelungen für die Nutzung von Datenträgern und Notebooks seiner Arbeitnehmer.
   - Der Auftragnehmer überprüft die schriftlichen Regelungen für die Nutzung von Datenträgern und Notebooks seiner Arbeitnehmer.
   - Die Dateisysteme von Xentral sind verschlüsselt mit FileVault MacOS.
3. Zugriffskontrolle, die sicherstellt, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können:
   - Der Zugriff auf die verarbeiteten Daten in Xentral erfolgen auf Grundlage des Need-

to-know-Prinzips.

- Der Auftragnehmer protokolliert die Datenverarbeitung in Xentral.
- Der Auftragnehmer überprüft regelmäßig die Einrichtung des Berechtigungskonzepts.

4. Weitergabekontrolle, mit der dafür gesorgt wird, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:
   - Der Datenaustausch im Rahmen von Xentral wird verschlüsselt mit FileVault MacOS.
   - Der Datenaustausch über Xentral wird im Webserver des Auftragnehmers protokolliert.
   - Daten auf physikalischen Datenträgern des Auftraggebers beim Auftragnehmer werden digitalisiert, verschlüsselt und anschließend verbleibend Datenträger vernichtet.
   - Datenfernzugriffe des Auftragnehmer werden nach Verschlüsselungsverfahren des Auftraggebers durchgeführt oder nach SSH-Standard des Auftragnehmers.
5. Eingabekontrolle, mit deren Hilfe nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
   - Datenverarbeitungsvorgänge in Xentral werden durch den Auftragnehmer protokolliert.
6. Auftragskontrolle, die dafür sorgt, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
   - Der Auftraggeber und seine Mitarbeiter werden durch die ihm überlassenen Zugangsdaten für das Ticket-Center für Xentral identifiziert.
7. Verfügbarkeitskontrolle, d.h. es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
   - Virenkontrolle für eingehende Dateien per Mail
   - Der Auftragnehmer unterhält ein Firewall-Konzept
   - Der Auftragnehmer führt regelmäßige Datensicherungen durch; Daten- sicherungen werden verschlüsselt gelagert.
8. Trennungskontrolle, die sicherstellt, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:
   - Es erfolgt eine Trennung per individuellen und passwortgeschützten Zugang durch die Xentrals-Instanz des Kunden, auf die der Auftragnehmer Zugang erhält.
   - Es besteht eine Trennung zwischen Entwicklungs-, Test- und Produktivsystem von Xentral.

C. Maßnahmen zur Verfügbarkeit der personenbezogenen Daten und um den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Siehe Ziff.

- B.7. Punkt 3

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- Datenschutzorganisation
- formalisierte Prozesse für Datenschutzvorfälle
- Weisungen des Auftraggebers werden dokumentiert
- SLAs für die Durchführung von Kontrollen

Anhang 2 – Vergütungsbedingungen und Preisliste

§ 1 Vergütungsbedingungen

(1) Soweit nicht anders angegeben, verstehen sich die angegebenen Preise jeweils zzgl. der gesetzlichen Mehrwertsteuer.

(2) Die Vergütung ist jeweils sofort nach Rechnungseingang zur Zahlung fällig.

(3) Der Kunde ist zur Geltendmachung eines Zurückbehaltungs- oder Aufrechnungsrechts nur insoweit berechtigt, wie die zugrunde liegende Gegenforderung rechtskräftig festgestellt ist oder nicht bestritten wird.

§ 2 Preisliste

(1) Sämtliche Leistungen des Auftragnehmers im Rahmen dieses Vertrags werden mit 125 €/ Stunde zzgl. Material und Spesen abgerechnet, soweit sie nicht bereits im Rahmen der Customer Care-AGB den bestellten Leistungen des Kunden abgegolten ist

(2) Reisekosten und Spesen des Auftragnehmers sind vom Auftraggeber separat zu vergüten, wenn beide Parteien das Erscheinen von Mitarbeitern des Auftragnehmers außerhalb des Geschäftssitzes des Auftragnehmers vereinbaren. Die Höhe der Reisekosten und Spesen richtet sich nach der Bestellung im Rahmen der Customer Care-AGB. Ist in Der Bestellung keine Regelung über die Höhe und Spesen getroffen, richtet sie sich nach Maßgabe der jeweils zum Zeitpunkt der Leistungserbringung geltenden aktuellen Preisliste von Xentral, abrufbar unter URL www.xentral.de/preisliste. Sofern keine Preisliste unter der vorbenannten URL zur Verfügung steht, gelten insbesondere die Reisekosten als Spesen vereinbart:

- Pkw: 50ct/km
- Bahn: 1. Klasse, ICE (oder entspr.)
- Flüge: Economyklasse

Anhang 5 – Subunternehmer

Subunternehmer	Kontaktdaten	Tätigkeit
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen Telefon: 07161 60692 50 Fax: 07161 60692 79 Mail: service@teamviewer.com	Service, Fernwartung
Anydesk Software GmbH	Rosenbergstr. 46 70176 Stuttgart Mail: info@anydesk.de	Service, Fernwartung
Amazon Web Services Inc.	410 Terry Avenue North Seattle WA 98109 United States aws.amazon.com Fax: +1 206 266-7010	Hosting, Infrastructure/ Plattform/Software as a Service (zusammen “SaaS”)
Timme Hosting GmbH & Co. KG	Ovelgönner Weg 43 21335 Lüneburg Deutschland Tel.: +49 (0) 4131 / 22 78 1-0 Fax: +49 (0) 4131 / 22 78 1-78 Mail: info@timmehosting.de	Hosting
Google Inc.	1600 Amphitheatre Parkway,Mountain View, CA 94043 USA Tel: +1 650 253 0000 Fax: +1 650 253 0001 Mail: support-de@google.com	Verarbeitung von Dokumenten, Tabellen, allg. Datenspeicher, kollaboratives Arbeiten
edudip GmbH	Jülicher Str. 306 52070 Aachen	Webinar-Plattform
BroadSoft Germany GmbH / Placetel	Lothringer Str. 56 50677 Köln	Telefonanlage
rapidmail GmbH	Augustinerplatz 2 79098 Freiburg i.Br.	Versendung von Newslettern