Vertrag zur Verarbeitung von Daten im Auftrag
(Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 DSGVO)

zwischen

Firma: _____
Name: _____
Straße: _____
PLZ / Ort: _____

zu den Verträgen zu der Kundenummer: _____

- Auftraggeber –

und

Serverprofis GmbH
Mondstr. 2-4
D-85622 Feldkirchen

- Auftragnehmer –

(gemeinsam nachfolgend: „die Parteien“)

1. Geltungsbereich und Ziel der Vereinbarung

Mit dieser Vereinbarung zur Verarbeitung von Daten im Auftrag (nachfolgend **AV-Vertrag** genannt) beabsichtigen die Parteien ihre datenschutzrechtlichen Rechte und Pflichten in Bezug auf die durch den Auftragnehmer im Auftrag des Auftraggebers verarbeiteten Daten zu regeln und somit die gesetzlichen Anforderungen, insbesondere des Bundesdatenschutzgesetzes („**BDSG**“) und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („**DSGVO**“) (vgl. dort die Anforderungen des Art. 28 Abs.3 DGVO), zu erfüllen.

Dieser AV-Vertrag findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers im Auftrag des Auftraggebers verarbeiten bzw. ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann.

2. Gegenstand und Dauer der Auftragsverarbeitung, Laufzeit

2.1. Dieser AV-Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien die sich aus den Tätigkeiten des Auftragnehmers im Zusammenhang mit den, im Rahmen der Leistungsbeschreibungen und der jeweiligen zwischen den Parteien geschlossenen vertraglichen Vereinbarungen (insbesondere Geschäftsbedingungen des Auftragnehmers, Bestellungen und (Einzel-)Verträge über individuelle Leistungen) beschriebenen Leistungen ergeben. Der

Auftragnehmer stellt insbesondere Webhosting-Dienstleistungen, Webserver und andere Server zur Verfügung, ferner damit verbundene Leistungen wie z.B. Webseiten, E-Mail, Domainregistrierungen und SSL-Zertifikate usw. Im Rahmen der mit dem Auftragnehmer vereinbarten Leistungen hat der Auftraggeber – je nach Tarif und vereinbartem Leistungsumfang – unter Nutzung u.a. z.B. eines Webservers, die Möglichkeit, Daten des Auftraggebers zu verarbeiten bzw. kann im Zuge der Leistungserbringung ein Zugriff des Auftraggebers auf personenbezogene Daten des Auftragnehmers nicht ausgeschlossen werden.

2.2. Gegenstand der vertraglichen Leistung des Auftragnehmers ist somit nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als Dienstleister im Bereich des Webhostings, des Supports bzw. der Administration von Server-Systemen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

2.3. Konkret betrifft dies die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den unter der Kundennummer des Auftraggebers zusammengefassten Bestellungen (nachfolgend „Hauptvertrag“ genannt) im Einzelnen beschriebenen Leistung ergeben.

2.4. Bei etwaigen Widersprüchen zwischen Leistungsbeschreibungen oder Regelungen in Einzelverträgen haben die Bestimmungen dieses AV-Vertrages Vorrang. Abweichende Regelungen haben nur dann Vorrang vor diesem AV-Vertrag, wenn sie ausdrücklich auf diesen AV-Vertrag Bezug nehmen.

2.5. Dieser AV-Vertrag gilt für die Dauer der unter der Kundennummer des Auftraggebers jeweils gebuchten Hauptverträge. Soweit durch den Auftragnehmer faktisch über die Laufzeit des AV-Vertrages hinaus personenbezogene Daten des Auftraggebers verarbeitet werden, gelten die vertraglichen Vereinbarungen zur Zweckbindung und Einhaltung der technischen und organisatorischen Maßnahmen fort.

3. Anwendungsbereich

3.1. Die Art der Verarbeitung von Daten des Auftraggebers umfasst grundsätzlich jede Art von mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, insbesondere 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 von Daten.

Die Zwecke der Verarbeitung von Daten sind alle für die Erbringung der vertraglichen Leistung erforderlichen und sich aus den Vereinbarungen zwischen den Parteien ergebenden Vertragszwecke.

3.2. Gegenstand der Auftragsverarbeitung, Art der Daten, Art und Zweck der Datenverarbeitung (Erhebung, Verarbeitung und Nutzung personenbezogener Daten) werden im Hauptvertrag ggfs. in Verbindung mit dazugehörigen Leistungsbeschreibung bzw. **Anlage 2** konkretisiert.

4. Rechte und Pflichten des Auftraggebers

4.1. Dem Auftraggeber ist bewusst, dass er im Rahmen des Hauptvertrages als verantwortliche Stelle („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO) alleine die Verantwortung für Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere die Verantwortung für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, sowie die Rechtmäßigkeit der Datenverarbeitung trägt.

4.2. Dem Auftraggeber steht die Weisungsbefugnis aus dem Hauptvertrag zu. Die Weisungen werden durch den Hauptvertrag festgelegt und können vom Auftraggeber in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werde („**Einzelanweisung**“). Weisungen die im Hauptvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich in Schriftform zu bestätigen.

4.3. Der Auftragnehmer weist dem Auftraggeber auf dessen Verlangen hin innerhalb angemessener Frist die Einhaltung seiner Pflichten nach diesem AV-Vertrag mit geeigneten Mitteln nach Wahl des Auftragnehmers nach, beispielsweise durch Durchführung eines Selbstaudits, Vorlage eines aktuellen Testats, durch Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) Zertifikate zum Datenschutz und/oder Informationssicherheit (z.B. nach BSI-Grundschutz oder ISO 270001) oder Zertifikate i.S.v. Art. 42 DSGVO. Hierfür entstehende Aufwendungen sind dem Auftragnehmer auf Basis seines zum jeweiligen Zeitpunkt gültigen üblichen Stundensatzes zu ersetzen, sofern zwischen den Parteien nichts Abweichendes vereinbart wurde.

4.4. Sollten im Einzelfall Kontrollen des Auftraggebers oder durch einen von diesem auf seine Kosten beauftragten Prüfers zur Einhaltung der Pflichten dieses AV-Vertrags, insbesondere der getroffenen technischen und organisatorischen Maßnahmen, erforderlich sein, werden diese zu den üblichen Geschäftszeiten des Auftragnehmers, ohne Störung dessen Betriebsablaufs nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf Kontrollmaßnahmen des Auftraggebers von der vorherigen Anmeldung mit angemessener Vorlaufzeit (mindestens 14 Tage) und Benennung mindestens dreier alternativer Termine sowie von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen, sofern nicht besondere Vorfälle eine davon abweichende Kontrolle rechtfertigen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Kontrollen des Auftraggebers vor Ort, sind - außer bei Vorliegen wichtiger datenschutzrechtlicher Gründe - grundsätzlich als Stichprobenkontrollen auszulegen und auf die Durchführung der Auftragsverarbeitung relevanten Bereiche und maximal auf einen Tag pro Kalenderjahr zu begrenzen.

4.5. Der Auftragnehmer ist berechtigt, dem Auftraggeber die für Kontrollmaßnahmen entstehenden Aufwendungen unter Zugrundelegung des zum jeweiligen Zeitpunkt gültigen Stundensatzes des Auftragnehmers in Rechnung zu stellen, sofern hierzu nichts Abweichendes zwischen den Parteien vereinbart wurde. Dies gilt auch für Inspektionen oder Kontrollen des Auftraggebers durch eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde.

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

4.7. Der Auftraggeber nennt dem Auftragnehmer einen ausreichend bevollmächtigten Ansprechpartner für sämtliche im Rahmen des AV-Vertrages anfallende Datenschutzfragen. Ein Wechsel des Ansprechpartners ist dem Auftragnehmer vom Auftraggeber unverzüglich mitzuteilen.

4.8. Sollte der Auftragnehmer durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüchen (insbesondere nach Art. 82 DSGVO) in Anspruch genommen werden, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

5. Pflichten des Auftragnehmers

5.1. Der Auftragnehmer darf Daten nur im Rahmen des in der jeweiligen Anlage 2 genannten Zwecks bzw. gemäß der Vereinbarungen im Hauptvertrag gemäß der Weisungen des Auftraggebers verarbeiten, sofern nicht ein gesetzlicher Ausnahmefall (z.B. nach Art. 28 Abs.3 lit.a DSGVO) vorliegt. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen anwendbare Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber schriftlich bestätigt oder geändert wird. Sofern der Auftragnehmer der Auffassung ist, dass eine weisungsgerechte Verarbeitung zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, ist er berechtigt die weitere Verarbeitung bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen. Zu einer materiell-rechtlichen Prüfung von Weisungen ist der Auftragnehmer nicht verpflichtet.

5.2. Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den Anforderungen des Datenschutzes im erforderlichen Maße gerecht wird. Hierfür wird der Auftragnehmer technische und organisatorische Maßnahmen zum angemessenen Schutz der im Auftrag des Auftraggebers verarbeiteten Daten treffen, die den Anforderungen des Art. 32 DSGVO genügen, insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung sicherstellen. Dem Auftraggeber sind diese Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese ein angemessenes Schutzniveau für das Risiko der mit dem Auftragnehmer vereinbarten Verarbeitungsvorgängen einhalten. Der Auftragnehmer wird um seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, die Wirksamkeit seiner technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüfen. Der Auftragnehmer ist berechtigt, die Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich ist, insbesondere die entsprechend Art. 32 DSGVO getroffenen Sicherheitsmaßnahmen jederzeit zu ändern, sofern sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

5.3. Der Auftragnehmer unterstützt den Auftraggeber auf dessen Weisung unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Der Auftragnehmer unterstützt den Auftraggeber auf dessen Weisung unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen ferner bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten. Der Auftragnehmer wird die hierfür jeweils bei Ihm vorhandenen notwendigen Information unverzüglich an den Auftraggeber weiterleiten. Für eine rechtzeitige Erfüllung der Pflicht des Auftraggeber zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechte oder Meldungen nach Art.

33 und 34 DSGVO ist der Auftragnehmer im Übrigen nicht verantwortlich. Der Auftragnehmer ist berechtigt, dem Auftraggeber die hierfür entstehenden Aufwendungen unter Zugrundelegung des zum jeweiligen Zeitpunkt gültigen Stundensatzes des Auftragnehmers in Rechnung zu stellen, sofern hierzu nichts Abweichendes zwischen den Parteien vereinbart wurde

5.4. Die vom Auftraggeber mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen werden vom Auftragnehmer auf die Wahrung des Datengeheimnisses verpflichtet. Den Mitarbeitern des Auftragnehmers wird dabei untersagt Daten des Auftraggebers außerhalb der Weisung zu verarbeiten und Daten des Auftraggebers vertraulich zu behandeln. Diese Vertraulichkeits-/ Verschwiegenheitspflicht sollen auch nach Beendigung des Auftrages fortbestehen.

5.5. Der Auftragnehmer nennt dem Auftraggeber auf Anforderung einen Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Soweit gesetzlich vorgeschrieben wird der Auftragnehmer einen Beauftragten für Datenschutz bestellen und dessen Kontaktdaten dem Auftragnehmer auf Anfrage zur Verfügung stellen. Ein Wechsel des Beauftragten für den Datenschutz bzw. des genannten Ansprechpartners für Datenschutzfragen ist dem Auftraggeber unverzüglich mitzuteilen.

5.6. 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.

5.7. 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.

5.8. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Der Auftragnehmer ist berechtigt, dem Auftraggeber die hierfür entstehenden Aufwendungen unter Zugrundelegung des zum jeweiligen Zeitpunkt gültigen Stundensatzes des Auftragnehmers in Rechnung zu stellen, sofern hierzu nichts Abweichendes zwischen den Parteien vereinbart wurde.

6. Technische und organisatorische Maßnahmen zum Datenschutz

6.1. Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der im Auftrag des Auftraggebers verarbeiteten Daten treffen, die den gesetzlichen Anforderungen genügen, insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung sicherstellen. Der als **Anlage 1** zu diesem AV-Vertrag beigefügte Katalog über technische und organisatorische Maßnahmen zum Schutz gegen unbefugtes Verarbeiten von Daten wird hierfür als verbindlich festgelegt und vom Auftragnehmer umgesetzt. Dem Auftraggeber sind diese Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese ein angemessenes Schutzniveau für das Risiko der mit dem Auftragnehmer vereinbarten Verarbeitungsvorgängen einhalten.

6.2. Der Auftragnehmer ist berechtigt, die Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich ist, insbesondere die entsprechend **Anlage 1** getroffenen Sicherheitsmaßnahmen jederzeit zu ändern, sofern sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Der Auftraggeber kann jederzeit eine aktuelle Fassung der von dem Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

7. Berichtigung, Löschung und Sperrung von Daten

7.1. Der Auftragnehmer hat nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren, sofern dies vom Weisungsrahmen des Auftraggebers 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. Der Auftragnehmer ist berechtigt, dem Auftraggeber die hierfür entstehenden Aufwendungen unter Zugrundelegung des zum jeweiligen Zeitpunkt gültigen Stundensatzes des Auftragnehmers in Rechnung zu stellen, sofern hierzu nichts Abweichendes zwischen den Parteien vereinbart wurde.

7.2. Nach Beendigung des Auftrages wird der Auftragnehmer auf Verlangen des Auftraggebers alle Daten löschen oder herausgeben. Der Auftragnehmer ist berechtigt, dem Auftraggeber die für eine Herausgabe der Daten bzw. die bei abweichenden Vorgaben des Auftraggebers für eine Herausgabe oder Löschung der Daten entstehenden Aufwendungen unter Zugrundelegung des zum jeweiligen Zeitpunkt gültigen Stundensatzes des Auftragnehmers in Rechnung zu stellen, sofern hierzu nichts Abweichendes zwischen den Parteien vereinbart wurde

8. Begründung von Unterauftragsverhältnissen

8.1. Die Begründung von Unterauftragsverhältnissen mit verbundenen Unternehmen oder Dritten (d.h. mit Dienstleistern, die den Auftragnehmer bei der Leistungserbringung unterstützen und dabei Zugriff bzw. Zugriffsmöglichkeit auf die Daten erhalten, z.B. Rechenzentren) ist dem Auftragnehmer jederzeit gestattet.

8.2. Der Auftragnehmer wird mit den Unterauftragnehmern Regelungen zur Auftragsdatenverarbeitung treffen, die mindestens den Anforderungen der vorliegenden Bedingungen entsprechen. Insbesondere wird der Auftragnehmer die Unterauftragnehmer verpflichten, die Weisungen des Auftraggebers zu beachten, ihm Informationen zu erteilen, erforderlichenfalls auch Einsicht in relevante Vertragsunterlagen zu geben. Kommerzielle Bedingungen dürfen in diesem Fall vom Auftragnehmer geschwärzt werden. Der Auftraggeber ist zur Geheimhaltung der gewonnenen Informationen verpflichtet und wird sich auf Anforderung des Auftragnehmers einer schriftlichen Geheimhaltungsvereinbarung unterwerfen.

8.3. Der Auftraggeber ist berechtigt, personenbezogene Daten des Auftragnehmers an Unterauftragnehmer in einem Drittland zu übermitteln, sofern die zwingenden gesetzlichen Vorschriften für Datenexporte in Drittländer erfüllt sind. Hierzu sind ferner dem Auftraggeber die erforderlichen Angaben und Informationen vorab zur Verfügung zu stellen, beispielsweise in Anlage 2 oder den jeweiligen zusätzlichen (Vertrags-) Unterlagen.

8.4. Nicht als Unterauftragsverhältnisse im Sinne Ziff. 8 sind solche Dienstleistungen zu verstehen, die der Auftragnehmer als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in

Anspruch nimmt (insbesondere Telekommunikationsdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer, die Entsorgung von Datenträgern oder sonstige externe Personal-, Post-, oder Versanddienstleistungen).

8.5. Auf Unter-Unterauftragsverhältnisse sind die Vorgaben zu Unterauftragsverhältnissen analog anwendbar und diesen entsprechend datenschutzrechtlich zu gestalten.

9. Anfragen betroffener Personen

9.1. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung seiner Daten oder Auskunft wenden sollte, 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 wird das Ersuchen des Betroffenen unverzüglich an den Auftraggeber weiterleiten.

9.2. Der Auftragnehmer wird den Auftraggeber auf dessen Weisung angemessen unterstützen, soweit dies für die Erteilung der Auskunft durch den Auftraggeber erforderlich ist. Dabei auf Seiten des Auftragnehmers entstehende Aufwendungen, werden gegen Ersatz dieser Aufwendungen unter Zugrundelegung seines jeweils gültigen Stundensatzes erbracht., sofern hierzu nichts Abweichendes zwischen den Parteien vereinbart wurde.

9.3. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

10. Haftung

10.1. Die zwischen den Parteien im Hauptvertrag getroffene Haftungsregelung gilt auch für die vorliegende Auftragsverarbeitung, sofern nicht ausdrücklich eine abweichende Vereinbarung getroffen wurde.

10.2. Soweit durch eine unzulässige oder unrichtige Datenverarbeitung im Rahmen dieses Auftragsdatenverarbeitungsverhältnisses ein Schaden entsteht und dieser Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist haftet hierfür alleine der Auftraggeber. Der Auftraggeber stellt den Auftragnehmer auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der konkreten Umsetzung der beauftragten Dienstleistung oder der vom Auftraggeber erteilten Weisung gegen den Auftragnehmer erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftraggeber dem Auftragnehmer ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

11. Beginn der Vereinbarung, Aufhebung bisheriger Vereinbarungen

11.1. Dieser Vertrag tritt mit Bestätigung des Vertragsschlusses durch den Auftraggeber, in Kraft. Die Bestätigung des Vertragsschlusses durch den Auftraggeber kann gemäß Art. 28 DSGVO in einem elektronischen Format erfolgen.

11.2. Die Parteien vereinbaren einvernehmlich, dass zeitgleich mit dem in Ziff. 11.1 genannten Beginn dieses Vertrages bisher zwischen den Parteien bestehenden Vereinbarungen zur Auftragsdatenverarbeitung im Sinne von § 11 BDSG einvernehmlich aufgehoben und durch den vorliegenden Vertrag ersetzt werden.

12. Schlussbestimmungen

12.1. Sollten das Eigentum des Auftraggebers, oder Gegenstände des Auftragnehmers die Daten des Auftraggebers enthalten, durch Maßnahmen Dritter (etwa Pfändungen oder Beschlagnahmungen) oder von Rechten Dritter (Sicherungsübereignung) betroffen sein, 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. Soweit möglich, sind alle Daten des Auftraggebers rechtzeitig vor Eintritt dieser Maßnahmen von den betroffenen Datenverarbeitungskomponenten zu entfernen.

12.2. Änderungen und Ergänzungen dieses AV-Vertrags 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.

12.3. Es gilt deutsches Recht. Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AV Vertrag ist München.

12.4. Sollte eine Bestimmung oder Teile dieses AV-Vertrags unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die Parteien verpflichten sich, anstelle der unwirksamen Bestimmung eine in sachlicher Hinsicht vergleichbare und am wirtschaftlichen Zweck des Vertrages orientierte, ersatzweise Regelung vereinbaren.

12.5. Die nachfolgend aufgezählten Anlagen werden zum Bestandteil dieses AV-Vertrags. Die jeweiligen Anlagen 2 sind von den Parteien separat zu vereinbaren:

Anlage 1: Technische und Organisatorische Maßnahmen nach Art. 32 DSGVO
Anlage 2: Beschreibungen der Auftragsverarbeitungen

Feldkirchen, 18.5.2018 _____, _____

Ort Datum

Serverprofis GmbH
Mondstr. 24
D-85622 Feldkirchen
Tel: +49 89 41615499-0
E-Mail: info@serverprofis.de

Martin Müller
Geschäftsleitung Serverprofis GmbH

_____

Unterschrift/Firmenstempel Auftraggeber

Anlage 1: Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

Zutrittskontrolle

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

Im Rechenzentrum:

- Zutritt nur über Anmeldung beim Rechenzentrum möglich
- Pförtner nimmt Besucher in Empfang
- Ausweiskontrolle / Berechtigungskontrolle und Eintragung in Besucherliste
- Biometrische Zugangserkennung durch Rechenzentrum Personal zu einzelnen Teilbereichen
- Personenvereinzelungsanlage mit Gewichtskontrolle
- Videoüberwachung des gesamten Rechenzentrums, inkl. des Eingangs und der der einzelnen Zonen/Rackreihen

In den Büroräumen des Auftragnehmers:

- Zugänge zu den Büroräumen grundsätzlich verschlossen
- Zentrales Schließsystem mit Sicherheitsschlössern
- Öffnen der Zugangstüren nur mit Schlüssel
- Besucherregelung: Abholung von Besuchern (nach Klingeln) am Eingang zum Bürotrakt
- Dokumentierte Verfahrensweise für Ausgabe und Rückgabe der Zugangsmittel
- Videoüberwachung der Büro Eingangsbereiche
- Alle Büroräume befinden sich im 2. OG

Zugangskontrolle

Es existieren folgende Maßnahmen zur Zugangskontrolle:

- Whitelising von zugelassen IP-Adressen
- Verschlüsselung der Home-Partitionen der DV-Geräte
- Zwei-Faktor-Authentifzierung Verschlüsselung für Kundenportal
- Zwei-Faktor-Authentifzierung für Kundensysteme bei Bedarf
- Firewall/IDS System
- Zugang zu DV-Geräten mit persönlicher Benutzernamen und Kennwort
- Kennwörter sofern möglich mit YubiKey abgesichert, ansonsten größer 12 Zeichen, bestehend aus Sonderzeichen, Groß-/Kleinbuchstaben sowie Zahlen und Sonderzeichen
- Protokollierung der Logins und Kennwortfehleingaben
- Verbindung zur Applikation im Rechenzentrum nur über VPN
- Einsatz von Anti-Viren-Software

Zugriffskontrolle

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- Benutzerrollen / Gruppenkonzept
- Überprüfung/Aktualisierung der Berechtigungen;
- Zeitgesteuerte Bildschirmsperre mit Wiederanmeldung
- Bildschirme so aufgestellt, dass ein unbefugtes Lesen verhindert wird
- Papier Shredder für Dokumentenvernichtung
- Keine externen EDV Dienstleister
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Administration der Systeme auf ein Minimum an Personal beschränkt.
- Zugriff für Mitarbeiter nach dem „Least to know“ Prinzip

Trennung

Es existieren folgende Maßnahmen zur Trennung von Daten:

- Trennung von Kundendaten durch separate Logins, welche vom Kunden vorgegeben werden, getrennt
- Trennung von Entwicklungs- und Produktionsumgebung

Pseudonymisierung & Verschlüsselung

- Es existieren keine Maßnahmen zur Pseudonymisierung.
- Passwörter werden in allen Systemen verschlüsselt gespeichert.

2. Integrität

Eingabekontrolle

Es existieren folgende Maßnahmen zur Eingabekontrolle:

- Protokollierung bei Eingabe, Änderung und Löschung von Daten
- Regelungen zum Zugriff und zur Löschung der Protokolle
- Nur Mitarbeiter mit der Rolle Administrator haben Zugriff auf die Protokolle

Weitergabekontrolle

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- Ausschließlich verschlüsselte Übertragung mit SSL/TLS Zertifikaten
- Identifizierung und Authentifizierungsverfahren
- Regelungen für die Datenträgervernichtung
- Die Löschung der Kundendaten sowie die Löschung der gebuchten Leistungen wird in einem Logfile dokumentiert.

Auftragskontrolle

Es existieren folgende Maßnahmen zur Auftragskontrolle:

- Mit allen Auftragnehmern wird bei Vorliegen der gesetzlichen Voraussetzungen ein AV Vertrag (gemäß Art. 28 DSGVO) abgeschlossen.
- Verschwiegenheitserklärungen der Mitarbeiter

3. Verfügbarkeit und Belastbarkeit

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

Im Rechenzentrum:

- Alle Server befinden sich in einem Rechenzentrum in Deutschland
- Alle Rechenzentren sind DiN ISO 27001 zertifiziert
- Redundante/Unterbrechungfreihe Stromversorgung durch USV / Dieselaggregate
- Redundante Netzteile in allen Servern ab Kaufdatum 2016
- Rauchmelder/ Löschanlagen (Argon)
- Überspannungsschutz
- IDS Systeme
- Alle Systeme werden mit redundanten RAID-Systemen ausgestattet
- Regelung durch Datensicherungskonzept
- Monitoring der Verfügbarkeit und Leistungskapazitäten der gesamten Infrastruktur
- Schutz gegen Feuer und Wassereintritt
- Virenscanner/Exploitscanner
- Ersatz und Austauschkomponenten vor Ort

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Verwendungszweckkontrolle)

Es existieren folgende Maßnahmen zur Verwendungszweckkontrolle:

- In regelmässigen Abstand von 1 Jahr, oder anlassbezogen auch früher, wird dies durch die Geschäftsführung überprüft.

Anlage 2: Beschreibung der Auftragsverarbeitung

1. Dauer und Gegenstand der Auftragsverarbeitung

Die Laufzeit des Auftrags ergibt sich aus den jeweiligen unter der Kundennummer des Auftraggebers bestehenden Bestellungen. Der Gegenstand des Auftrages ergibt sich aus den unter der Kundennummer des Auftraggebers zusammengefassten Verträgen.

2. Art der Daten, Art und Zweck der Datenverarbeitung sowie Betroffene

Alle Daten die der Auftraggeber, oder von ihm autorisierte Nutzer, im Rahmen der von ihm genutzten Dienste, beim Auftragnehmer speichert (Inhalt von Webseiten, Online-Speicher, Datenbanken usw.). Betroffen sind hiervon folgende Datenarten/Datenkategorien (Bitte zutreffendes ankreuzen, Mehrfachbenennungen sind möglich):
[Vom Auftraggeber vollständig und wahrheitsgemäß auszufüllen]

- ☐ Abrechnungsdaten
- ☐ Adressdaten
- ☐ Authentifizierungsdaten
- ☐ Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Bankverbindungsdaten
- ☐ Bestelldaten
- ☐ Bilddaten
- ☐ Empfänger und Versender von Nachrichten (z.B. Emails), die an den Auftraggeber gerichtet sind oder von dieser ausgehen sowie entsprechende Inhaltsdaten der Nachrichten
- ☐ Kundenhistorie
- ☐ Mitarbeiterdaten, Personaldaten
- ☐ Nutzungsdaten, z.B. Log-Dateien (insb. Namen von Nutzern von IT-Systemen oder Anwendungen, IP-Adressen)
- ☐ Planungs- und Steuerungsdaten
- ☐ Programmcode
- ☐ Stammdaten
- ☐ Systemzugangsdaten, Passwortdateien
- ☐ Transaktionsdaten
- ☐ Wirkdaten der Systeme des Auftraggebers (Produktions- und Echtdaten)
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Vertragsstammdaten (Angebotsdaten, Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Videodateien
- ☐ Sonstige Daten (bitte aufzählen):

Betroffen von der Speicherung ihrer Daten sind folgende Kategorien von Personen
(Bitte Zutreffendes ankreuzen, Mehrfachbenennungen sind möglich):
[Vom Auftraggeber vollständig und wahrheitsgemäß auszufüllen]

- ☐ Abonnenten
- ☐ Angehörige

- ☐ Auszubildende
- ☐ Bewerber
- ☐ Berater
- ☐ Dienstleister
- ☐ Empfänger und Versender von Nachrichten, die an den Auftraggeber gerichtet sind oder von ihm ausgehen
- ☐ Geschädigte
- ☐ Geschäftspartner
- ☐ Gesellschafter
- ☐ Handelsvertreter
- ☐ Interessenten
- ☐ Kunden
- ☐ Lieferanten
- ☐ Makler / Vermittler
- ☐ Mandanten
- ☐ Mitarbeiter (aktiv)
- ☐ Mitarbeiter (ehemalige)
- ☐ Mitglieder
- ☐ Nutzer
- ☐ Patienten
- ☐ Praktikanten
- ☐ Sonstige Betroffene (bitte aufzählen): ……

  ……

  ……...

4. Verantwortlichkeiten

Als weisungsberechtigten Ansprechpartner des Auftraggebers gelten die im Kundenportal des Auftragnehmers hinterlegten Kontaktpersonen.

Zuständige Weisungsempfänger des Auftragnehmers:

Organisationseinheit	**Telefon**	**E-Mail**
Support-Team	+49(89) 41615499-5	hotline@serverprofis.net

Änderungen der weisungsberechtigten oder -empfangenden Personen werden die Parteien (a) unverzüglich anzeigen und (b) die Anlage 2 bzw. den Eintrag im Kundenportal des Auftragnehmers entsprechend anpassen.

5. Ort der Datenverarbeitung (Mehrfachnennungen möglich)

Deutschland