Vereinbarung zur Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

abgeschlossen zwischen

Nutzer/-in der SEKTOR7 Dienste

- Nachstehend Auftraggeber genannt -

und der

SEKTOR7 – Schlotte & Feilke GbR
Hauptstraße 25 in 18546 Sassnitz

- Nachstehend Auftragnehmer genannt -

I Versionsstände

Version	Datum	Kommentar	Bearbeiter
1	10.04.2018	Erstfassung	Martin Feilke
1.1	30.04.2018	Korrektur der Erstfassung	Martin Feilke

Tabelle 1: Versionsstände

§1 Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Vertragsverhältnis in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§2 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertragsverhältnisses, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

§3 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung 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 DSGVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt

werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§4 Pflichten des Auftragnehmers

(1) 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) DSGVO 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.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(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.

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

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen: SEKTOR7 IT-Systemhaus | Datenschutz | Martin Feilke | Hauptstraße 25 in 18546 Sassnitz | datenschutz@sektor7.com | 038392-659010

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) 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 Grund einer Einzelbeauftragung

durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) 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.

§5 Pflichten des Auftraggebers

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

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §4 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§6 Anfragen betroffener Personen

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

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(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. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(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 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist zulässig.
(2) Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.
(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.
(4) Beispielhaft seien hier Lieferanten und Cloudanbieter zu nennen. Eine vollständige Auflistung der beim Auftraggeber eingesetzten Subunternehmer kann jederzeit angefordert werden.

§9 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber 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.
(2) Änderungen und Ergänzungen dieser Vereinbarung 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.
(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
(4) Es gilt deutsches Recht.

§10 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§11 Technisch-Organisatorische-Maßnahmen

Die Allgemeinen Vorgaben für die Umsetzung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO finden Sie als Anlage beigefügt.

§12 Datenschutzerklärung

Die Datenschutzerklärung des Auftragsnehmers finden Sie unter folgendem Weblink: https://sektor7.com/rechtliches

Auftragsbestätigung

Durch das Akzeptieren der Auftragnehmer AGB, den Besonderen Geschäftsbedingungen für Managed Services und der Datenschutzerklärung des Auftragsnehmers stimmt der Auftraggeber dieser Vereinbarung zur Auftragsdatenverarbeitung mit der SEKTOR7 – Schlotte & Feilke GbR automatisch zu. Infolgedessen bedarf diese Vereinbarung keiner gesonderten Unterschrift um in Kraft zu treten.

Sassnitz, im April 2018 SEKTOR7 – Schlotte & Feilke GbR

Anlage: Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Ziel der **Zutrittskontrolle** ist es, dass Unbefugten der Zutritt zu solchen Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogener Daten verarbeitet oder genutzt werden. Es existieren folgende Maßnahmen zur Zutrittskontrolle:
  (1) Festlegung von Sicherheitsbereichen
  (2) Realisierung eines wirksamen Zutrittsschutzes
  (3) Festlegung zutrittsberechtigter Personen
  (4) Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
  (5) Begleitung von Besuchern und Fremdpersonal
  (6) Überwachung der Räume außerhalb der Schließzeiten
- Ziel der **Zugangskontrolle** ist es, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden, mit denen die Verarbeitung und Nutzung personenbezogener Daten durchgeführt werden. Es existieren folgende Maßnahmen zur Zugangskontrolle:
  (1) Zugangsschutz (Authentisierung)
  (2) Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
  (3) Gesicherte Übertragung von Authentisierungsgeheimnissen im Netzwerk
  (4) Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
  (5) Verbot von Speicherfunktionen für Passwörter und/oder Formulareingaben
  (6) Festlegung befugter Personen
  (7) Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
  (8) Dort wo technisch möglich, wird eine Zwei-Faktor-Authentifizierung eingesetzt
  (9) Verschlüsselung von Datenträgern
- Die Maßnahmen zur **Zugriffskontrolle** müssen darauf gerichtet sein, dass nur auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es existieren folgende Maßnahmen zur Zugriffskontrolle:
  (1) Berechtigungskonzept aller Mitarbeiter und Beauftragte
  (2) Umsetzung von Zugriffsbeschränkungen
  (3) Vergabe minimaler Berechtigungen
  (4) Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
  (5) Vermeidung der Konzentration von Funktionen
- Ziel der **Verwendungszweckkontrolle (Trennungskontrolle)** ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Es existieren folgende Maßnahmen zur Verwendungszweckkontrolle:
  (1) Getrennte Verarbeitung durch Ordnertrennung
  (2) Mandantenfähigkeit
- **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen

unterliegen.

2. **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**
   - Ziel der **Weitergabekontrolle** ist es, zu gewährleisten, 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Es existieren folgende Maßnahmen zur Weitergabekontrolle:
     (1) Protokollierungen jeder Übermittlung oder einer repräsentativen Auswahl
     (2) Sichere Datenübertragung zwischen Server und Client
     (3) Sicherung der Übertragung im Backend
     (4) Sicherung der Übertragung zu externen Systemen
     (5) Risikominimierung durch Netzseparierung
     (6) Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
     (7) Sichere, verschlüsselte Ablage von Daten
     (8) Verhinderung von Zugriffen auf lokale Zwischenspeicher
     (9) Sichere Datenträgeraufbewahrung
     (10) Prozess zur Sammlung und Entsorgung
     (11) Datenschutzgerechtes Lösch-/Zerstörungsverfahren
     (12) Notwendige Fernzugriffe erfolgen gesichert

   - Ziel der **Eingabekontrolle** ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass nachträglich die näheren Umstände der Dateneingabe überprüft und festgestellt werden können. Es existieren folgende Maßnahmen zur Eingabekontrolle:
     (1) Dokumentation der Eingabeberechtigungen

3. **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**
   - Ziel der **Verfügbarkeitskontrolle** ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:
     (1) Backup-Konzept
     (2) Notfallplan
     (3) Aufbewahrung der Backups
     (4) Einsatz unterbrechungsfreier Stromversorgungen
     (5) Einsatz von Virenschutz-Programmen
     (6) Einsatz von Firewall-Lösungen
     (7) Prüfung der Notfalleinrichtungen
   - Rasche Wiederherstellbarkeit

4. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**
   - Datenschutz-Management;
   - Incident-Response-Management;
   - Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
   - Ziel der **Auftragskontrolle** ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können. Es existieren folgende Maßnahmen zur Auftragskontrolle:
     (1) Protokollierung der Auftragsausführung durch den Auftragnehmer
     (2) Beschränkung der Auftragsausführung
     (3) Eindeutige Vertragsgestaltung

5. **Löschung von Festplatten, USB-Sticks, wiederbeschreibbare Datenträger**
   Für personenbezogene Daten (z.B. Kundendaten, Mitarbeiterdaten, etc.) auf Festplatten, USB-Sticks und anderen wiederbeschreibbaren Datenträgern kann jeweils eine der nachfolgend

aufgeführten Löschverfahren für eine datenschutzgerechte Löschung bis zur Datenschutzklasse 3, dies ist die höchste Datenschutzklasse, angewendet werden:

- Gutmann-Methode (35-maliges Überschreiben)
- DoD 5220 M (9-maliges Überschreiben)
- Deutscher Standard: VSITR
- Verfahren nach der Bruce Schneier Algorithmus (7-maliges Überschreiben)

Nicht geeignet sind die folgenden Methoden:

- DoD Short
- QuickErase
- DSX-Verfahren der kanadischen Bundespolizei
- FormatierenderFestplatte
- Neupartitionierung der Festplatte
- Wechselmagnetfeld als einzige Maßnahme

Zusätzlich wird vereinbart, die Festplatte zur oben beschriebenen Löschung noch durch ein starkes Wechselmagnetfeld zu ziehen, soweit dies möglich ist, damit Sektoren, die als fehlerhaft markiert sind, zumindest nicht einfach wieder herstellbar sind.

Defekte Datenträger oder Datenträger, bei denen eine Löschung technisch nicht bzw. nicht mehr möglich ist, müssen üb er den Auftraggeber datenschutzgerecht entsorgt werden (dürfen insbesondere nicht über den Hausmüll, den Hersteller oder Dritte entsorgt werden) oder mit dem Auftraggeber muss eine andere datenschutzgerechte Vorgehensweise vereibnart werden.

6. Löschung von Dateien auf Festplatten, USB-Sticks oder sonstigen wieder beschreibbaren Datenträgern

Unter Anwendung einer vorstehend als geeignet aufgeführten Methoden zur Löschung auf die einzelnen Dateien, die Kundendaten beinhalten, kann eine datenschutzgerechte Löschung sichergestellt werden.

Nicht geeignet sind folgende Methoden:

- Löschung mittels der Lösch-Taste (Delete- Funktion)
- Verschieben der Datei in den Papierkorb
- Umbenennen der Datei

Defekte Datenträger oder Datenträger, bei denen eine Löschung technisch nicht bzw. nicht mehr möglich ist, müssen über den Auftraggeber datenschutzgerecht entsorgt werden (dürfen insbesondere nicht über den Hausmüll, den Hersteller oder Dritte entsorgt werden) oder mit dem Auftraggeber muss eine andere datenschutzgerechte Vorgehensweise vereinbart werden.

7. Änderungen

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.