Vereinbarung zur Verarbeitung von Daten im Auftrag

zwischen

Firma, juristische oder natürliche Person
Straße, Hausnummer
PLZ Ort
Land

– Verantwortlicher –

und

soft.works, Raphael Boos
Gängle 11
88131 Lindau
– Auftragsverarbeiter –

Präambel

Führt ein Auftragsverarbeiter Leistungen im Auftrag seines Vertragspartners (Verantwortlicher) aus, müssen die Anforderungen der jeweils gültigen Datenschutzgesetze Berücksichtigung finden und insbesondere bei den Verarbeitungstätigkeiten ein angemessenes Datenschutzniveau garantiert sein. Die vorliegende Vereinbarung berücksichtigt die besonderen Anforderungen aus der EU-Datenschutzgrundverordnung[1].

[1] Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DatenschutzGrundverordnung, EU-DSGVO).

§ 1 Gegenstand des Auftragsverarbeitungsvertrages, Art. 28 Abs. 1 DSGVO

(1) Der Verantwortliche beauftragt den Auftragsverarbeiter mit der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten.

(2) Der Gegenstand des Auftrags und damit der Zweck, die Art und der Umfang der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten:
(Vom Verantwortlichen richtig auszufüllen und anzukreuzen)

☐ ergibt sich aus dem zugrunde liegenden Hauptvertrag:
Auftragsdatum:
Auftragsnummer:
Kundennummer:

☑ ist die Durchführung der folgenden Aufgabe(n) durch den Auftragsverarbeiter:

☑ **Webhosting** und damit zusammenhängende vertraglichen Leistungen wie Domainregistrierung, Zertifikate, E-Mail, FTP, Datenbanken, etc.

☑ **Erstellung und Betreuung von Webseiten** und der damit zusammenhängende Zugang zu weiteren Systemen des Verantwortlichen wie z.B. soziale Medien, Zahlungsdienste oder andere Dienste Dritter.

☑ **Webmarketing** und der damit zusammenhängende Zugang zu Systemen des Verantwortlichen für z.B. Konten für soziale Medien, Tools wie Adwords, Bing, Newsletter Systeme.

☐ ist die (Fern-)Wartung von Systemen, wobei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Gegenstand des Vertrages ist **nicht** die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter. Im Zuge der Leistungserbringung des Auftragsverarbeiters als zentraler Dienstleister im Bereich des Hostings, der Webseitenerstellung, des Webmarketings, des Supports, der Administration von Server-Systemen des Verantwortlichen, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

(4) Soweit nachfolgend von Daten die Rede ist, handelt es sich ausschließlich um personenbezogene Daten im Sinne der DSGVO. Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 Abs. 1 DSGVO, die der Auftragsverarbeiter gegenüber dem Verantwortlichen erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können.

(5) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede nicht in diesem Vertrag gesondert aufgeführte Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der einschlägigen Datenschutzgesetze erfüllt sind.

(6) Squarespace Websites / USA
Falls für Webseiten das Redaktionssystem „Squarespace.com“ genutzt wird: dieses wird bereitgestellt von Squarespace, Inc., 225 Varick Street, 12th Floor, New York, NY 10014, EU-MWST-Nr.372003935 (im Folgenden Squarespace). Squarespace erfüllt die Bedingungen des EU-US und US-SWISS Privacy Shield Abkommens. Details finden Sie hier:
https://www.privacyshield.gov/participant?id=a2zt0000000GnjcAAC
https://support.squarespace.com/hc/en-us/articles/360000851908-GDPR-and-Squarespace

(7) ECWID Shopping Carts / USA
Falls Sie auf Ihrer Website das E-Commerce Plugin „ECWID“ nutzen: Betreiber des Plugins ist ECWID Inc., 144 West D Street, Suite 103, Encinitas, CA 92024 USA (im Folgenden ECWID). ECWID erfüllt die Bedingungen des EU-US und US-SWISS Privacy Shield Abkommens. Details finden Sie hier:
https://www.privacyshield.gov/participant?id=a2zt0000000GnCfAAK
https://support.ecwid.com/hc/en-us/articles/360000608449-General-Data-Protection-Regulation-GDPR-and-Ecwid-stores

§ 2 Dauer, Laufzeit der Auftragsverarbeitung

(Vom Verantwortlichen richtig auszufüllen und anzukreuzen)

- ○ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages.
- ○ Der Auftrag wird zur einmaligen Ausführung erteilt.
- ○ Der Auftrag wird bis zum erteilt.
- ◉ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 3 Monat(en) zum Quartalsende gekündigt werden, sofern keine abweichende Kündigungsfrist vereinbart wurde. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 3 Art der Daten

Gegenstand der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten sind Daten der folgenden Datenartenkategorien:

(Vom Verantwortlichen richtig auszufüllen und anzukreuzen)

- ☐ Abrechnungsdaten z.B. Verbrauchs, - Leistungswerte
- ☐ Arbeitszeitdaten
- ☐ Bewerberdaten
- ☐ Biometrische Daten
- ☐ Bonitätsdaten, z.B. Scoring, Zahlungshistorie
- ☐ Gehalts- und Lohndaten
- ☐ Genetische Daten
- ☐ Gesundheitsdaten
- ☐ Internetnutzungsdaten, z.B. IP-Adresse, Uhrzeit, Browser, Referer
- ☐ Interessensdaten
- ☐ Kontaktdaten
- ☐ Mitarbeiterdaten
- ☐ Protokolldaten, z.B. Logfiles über Nutzungsvorgänge eines Benutzers
- ☐ Schadensdaten
- ☐ Sozialversicherungsdaten
- ☐ Teilnehmerdaten
- ☐ Verbindungsdaten, z.B. Dauer, Zeit, Verbindungsteilnehmer Telefon
- ☐ Verhaltensdaten, z.B. Bewegungsprofile
- ☐ Versicherungsdaten

☐ Vertragsdaten

☐ Videoaufzeichnungen, z.B. Überwachungsdaten

☐ Zeiterfassungsdaten

☐ Sonstige, bitte angeben:

§ 4 Kreis der Betroffenen

Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen, umfasst folgende Kategorien:

(Vom Verantwortlichen richtig auszufüllen und anzukreuzen)

☐ Gäste

☐ Interessenten

☐ Kunden

☐ Abonnenten

☐ Lieferanten

☐ Dienstleister

☐ Partner

☐ Bewerber

☐ Beschäftigte / Rentner

☐ Teilnehmer

☐ Passanten

☐ Sonstige Betroffene:

§ 5 Technisch-organisatorische Maßnahmen, Art 32 DSGVO

(1) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben (**Anlage „Technisch-organisatorische Maßnahmen“**). Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Die technisch-organisatorischen Maßnahmen sollen die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie die Systembelastbarkeit im Zuge der Datenverarbeitung sicherstellen. Aus den

angegebenen Maßnahmen muss ein angemessenes Sicherheitsniveau ableitbar sein. Der Auftragsverarbeiter hat den Verantwortlichen bei der Ergreifung technisch-organisatorischer Maßnahmen bestmöglich zu unterstützen.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 6 Berichtigung, Sperrung, Einschränkung und Löschung von Daten

Der Auftragsverarbeiter hat nur nach Weisung des Verantwortlichen die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen, einzuschränken oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

§ 7 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags folgende Pflichten:

a) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.

b) Die Wahrung des Datengeheimnisses. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Verantwortlichen zugreifen können, müssen auf das Datengeheimnis und die Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

c) Die Wahrung des Fernmeldegeheimnisses nach § 88 TKG. Alle Personen, die auftragsgemäß auf Inhalte von Telekommunikation zugreifen können, müssen auf das Fernmeldegeheimnis verpflichtet und über die sich auf diesem Auftrag ergebenden besonderen Schutzpflichten sowie die bestehende Zweckbindung belehrt werden.

d) Der Auftragsverarbeiter stellt sicher, dass er die Verarbeitung personenbezogener Daten ausschließlich auf Grundlage dokumentierter Weisungen des Verantwortlichen im Sinne dieses Vertrages vornimmt. Sofern der Auftragsverarbeiter zu einer Verarbeitung gesetzlich verpflichtet ist, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

e) Der Auftragsverarbeiter hat den Verantwortlichen bei seiner Pflicht zur Wahrung der Betroffenenrechte zu unterstützen. Dies ist durch geeignete organisatorische Maßnahmen zu gewährleisten.

f) Der Auftragsverarbeiter ist verpflichtet, im Rahmen seiner Tätigkeit für den Verantwortlichen an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an den Verantwortlichen weiterzuleiten. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Verantwortlichen selbständig zu bescheiden.

g) Sofern den Verantwortlichen aufgrund eines voraussichtlich hohen Risikos der Verarbeitung die Pflicht zur Datenschutz-Folgenabschätzung trifft, hat der Auftragsverarbeiter ihn hierbei zu unterstützen. Dies gilt ebenso für die Pflicht zur vorherigen Konsultation der Aufsichtsbehörde, sofern sich eine solche aus der vorangegangenen Folgenabschätzung ergibt.

h) Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde beim Auftragsverarbeiter ermittelt.

i) Soweit den Verantwortlichen Pflichten nach Art. 32 und 33 DSGVO treffen, hat der Auftragsverarbeiter ihn hierbei zu unterstützen. Soweit den Verantwortlichen Pflichten nach Art. 32-36 DSGVO treffen, z.B. im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten durch Dritte, hat der Auftragsverarbeiter ihn hierbei im Rahmen des Charakters der durch den Auftragsverarbeiter erbrachten Dienstleistung zu unterstützen.

§ 8 Unterauftragsverhältnisse des Auftragsverarbeiters

(1) Der Verantwortliche ist damit einverstanden, dass der Auftragsverarbeiter zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich, für die Bereiche Hosting, Servermanagement, Serverwartung, Rechenzentrumsinfrastruktur, Cloud Computing, SAAS Services Unterauftragsverarbeiter zur Leistungserfüllung heranzieht.

(2) Erteilt der Auftragsverarbeiter Aufträge an Unterauftragsverarbeiter, so obliegt es dem Auftragsverarbeiter, seine Pflichten aus diesem Auftragsverarbeitungsvertrag dem Unterauftragsverarbeiter zu übertragen. Es müssen hinreichende Garantien dafür geboten sein, dass die technischen und organisatorischen Maßnahmen den Anforderungen an die rechtmäßige Datenverarbeitung genügen

(3) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt.

Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer etc. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(4) Die Auftragsverarbeiter trägt dafür Sorge, dass dem Verantwortlichen eine aktuelle Liste der eingesetzten Unterauftragsverarbeiter zur Verfügung steht. Bei Änderung dieser Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Unterauftragsverarbeitern ergeht hierüber eine Information an den Verantwortlichen.

(5) Der Auftragsverarbeiter setzt folgende(n) Unterauftragsverarbeiter zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Sinne dieser Vereinbarung ein:
(Vom Auftragsverarbeiter richtig auszufüllen und anzukreuzen)

☑ **OWIS - Hosting**
GRONEMEYER IT GmbH, Konrad-Zuse-Str. 1, D-37671 Höxter, www.owis.de

☐ **SQUARESPACE CMS System – Hosting, SAAS**
Bei Nutzung von Squarespace und Hosting Vertrag mit dem Auftragsverarbeiter. Squarespace, Inc., 225 Varick Street, 12th Floor, New York, NY 10014. Squarespace erfüllt die Bedingungen des EU-US und US-SWISS Privacy Shield Abkommens. Details finden Sie hier: https://www.privacyshield.gov/participant?id=a2zt0000000GnjcAAC

☐ Sonstiger Unterauftragsverarbeiter, bitte angeben:

§ 9 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, eine Auftragskontrolle mit dem Auftragsverarbeiter durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

(2) Im Hinblick auf die Kontrollverpflichtungen des Verantwortlichen vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragsverarbeiter sicher, dass sich der Verantwortliche von der Einhaltung der

getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragsverarbeiter dem Verantwortlichen auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI Grundschutz) oder durch andere hinreichende Garantien erbracht werden.

§ 10 Pflichten des Verantwortlichen, Art 13,14, 24 DSGVO

(1) Der Verantwortliche ist für die Einhaltung der für ihn einschlägigen datenschutzrechtlichen Regelungen verantwortlich.

(2) Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er Verstöße des Auftragsverarbeiters gegen datenschutzrechtliche Bestimmungen feststellt.

(3) Den Verantwortlichen treffen die sich aus Art. 24 DSGVO und Art. 13 und 14 DSGVO ergebenden Informationspflichten.

(4) Die Rechte der durch den Datenumgang bei dem Auftragsverarbeiter betroffenen Personen, insbesondere auf Berichtigung, Löschung und Sperrung, sind gegenüber dem Verantwortlichen geltend zu machen. Er, der Verantwortliche, ist allein verantwortlich für die Wahrung dieser Rechte.

(5) Der Verantwortliche hat selbst jederzeit umfassenden Zugriff auf die Daten, so dass es einer Mitwirkung des Auftragsverarbeiters insbesondere auch zu Berichtigung, Sperrung, Löschung etc. nicht bedarf. Soweit eine Mitwirkung des Auftragsverarbeiters erforderlich ist, ist der Verantwortliche hierzu gegen Erstattung der anfallenden Kosten verpflichtet. Diesbezügliche Anfragen sind schriftlich an den Auftragsverarbeiter zu richten.

§ 11 Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter erstattet in allen Fällen dem Verantwortlichen eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Verantwortlichen oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

(2) Es ist dem Auftragsverarbeiter bekannt, dass Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind

solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Verantwortlichen mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Verantwortlichen. Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

(3) Soweit den Verantwortlichen Melde- und/oder Benachrichtigungspflichten treffen, hat der Auftragsverarbeiter ihn hierbei zu unterstützen. Dies gilt sowohl für die Meldung einer etwaigen Pflichtverletzung gegenüber der Aufsichtsbehörde, als auch für die Benachrichtigung der von der Verletzung des Schutzes personenbezogenen Daten betroffenen Personen.

§ 12 Weisungsbefugnis des Verantwortlichen

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Verantwortlichen. Der Verantwortliche behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

(2) Mündliche Weisungen wird der Verantwortliche unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch eine beim Verantwortlichen befugte Person bestätigt oder geändert wird.

§ 13 Löschung von Daten

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Als Aushändigung gilt auch die Möglichkeit, dass der Kunde sich die Daten selbst verschaffen kann. Zum Beispiel bekommt der Verantwortliche beim Hosting Werkzeuge, mit denen er sich die Daten selbst beschaffen kann. Wird der Auftragsverarbeiter hierfür herangezogen, können zusätzliche Kosten entstehen, die vom Verantwortlichen zu tragen sind.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

§ 14 Informationspflichten, Schriftformklausel, Rechtswahl, Salvatorische Klausel, Gerichtsstand

(1) Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung 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) Es gilt deutsches Recht sowie das in Deutschland unmittelbar und zwingend anzuwendende Recht der Europäischen Union.

(4) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.

(5) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der (datenschutz-

rechtlichen) Zielsetzung am nächsten kommen, welche die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.

(6) Als Gerichtsstand wird Lindau am Bodensee vereinbart.

Ort, Datum	Vorname, Name (Druckbuchstaben)	Stempel/ Unterschrift Verantwortlicher

Ort, Datum	Vorname, Name (Druckbuchstaben)	Stempel/ Unterschrift Auftragsverarbeiter

Anlage: Technisch organisatorische Maßnahmen

Technische und organisatorische Maßnahmen

von

soft.works, Raphael Boos
Gängle 11
88131 Lindau

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen technische und organisatorische Maßnahmen getroffen werden, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen.

Fachverantwortlicher für diese Maßnahmen: Raphael Boos

M.1 Maßnahmen zur Vertraulichkeit:

M.1.1 Beschreibung der Zutrittskontrolle:

- Einsatz einer Alarmanlage
- Bewegungsmelder
- Schließsystem mit PIN Codesperre
- Videoüberwachung des Zugangs

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort
- Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt)
- Einsatz von Firewalls zum Schutz des Netzwerkes

M.1.3 Beschreibung der Zugriffskontrolle:

- Erstellung und Einsatz eines Berechtigungskonzepts
- Sichere Löschung von Datenträgern vor deren Wiederverwendung
- Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2)
- Passwortrichtlinie inkl. Länge, Komplexität
- Sichere Aufbewahrung von Datenträgern

M.1.4 Beschreibung der Weitergabekontrolle:

- Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
- Einsatz von SSH bei Verbindung zu Serverkonsolen
- Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem

M.1.6 Beschreibung der Pseudonymisierung:

- Trennung von Kontaktdaten und anderen Daten
- Trennung von Kundenstammdaten und Auftragsdaten

M.1.7 Beschreibung der Verschlüsselung:

- Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard)
- Verschlüsselte Datenübertragung (z.B. E-Mailverschlüsselung nach PGP oder S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL)

M.2 Maßnahmen zur Integrität:

M.2.1 Beschreibung der Eingabekontrolle:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit:

- Einsatz von Antivirensoftware zum Schutz vor Malware
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- & Recoverykonzepts
- Feuer- und Rauchmeldeanlagen
- Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher)
- Schutzsteckdosenleisten
- (USV) Unterbrechungsfreie Stromversorgung

M.3.2 Beschreibung der Wiederherstellbarkeit:

- Regelmäßige und dokumentierte Datenwiederherstellungen

M.4 Weitere Maßnahmen:

M.4.1 Beschreibung der Auftragskontrolle:

- Auswahl von Auftragnehmern und Unterauftragsverarbeitern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schulungen aller zugriffsberechtigten Mitarbeiter und Nachschulungen.

- Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO

M.4.2 Beschreibung des Managementsystems:

- Managementsystem zum Datenschutz (Audatis)

Lindau, 10.05.2018 Raphael Boos

Ort, Datum

Befugte Person (in Druckbuchstaben)

Unterschrift der befugten Person