Vereinbarung zur Auftragsverarbeitung

gem. Art. 28 DSGVO

Zwischen dem

Beraterkunden (Verantwortlicher)

vertreten durch die Geschäftsführung / den Vorstand

- nachfolgend auch **Beraterkunde** genannt -

und der

SMARTCON Wirtschaftsberatung GmbH & Co. KG (Auftragsverarbeiter)

Bartholomäusstraße 26D, 90489 Nürnberg,
vertreten durch die Geschäftsführung

- nachfolgend auch **smartcon** genannt -

wird nachfolgender Auftragsverarbeitungsvertrag geschlossen.

Präambel

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht bei Buchung der Software *verfahrensdokumentation.pro* (bzw. anderer angebotener Softwarelösungen) ein vorvertragliches Schuldverhältnis und anschließend ein Vertragsverhältnis über die Nutzung der gebuchten Software (im Weiteren: Softwarevertrag)

Im Rahmen des Softwarevertrags stellt der Auftragsverarbeiter dem Verantwortlichen eine internetbasierte Software (als Software as a Service) zur Verfügung, mit der dieser Verfahrensdokumentationen für seine Auftraggeber (im Weiteren: Mandanten) erstellen kann. Im Rahmen der Softwarenutzung verarbeitet der Verantwortliche gegebenenfalls auch personenbezogene Daten seiner Mitarbeiter und seiner Mandanten.

Der Verantwortliche ist eigenständiger Verantwortlicher im datenschutzrechtlichen Sinne, soweit er Fachleistungen gegenüber den Mandanten erbringt, bei denen er berufsrechtlich zum besonderen Schutz personenbezogener Daten verpflichtet ist (insbesondere als Steuerberater, Rechtsanwalt oder Wirtschaftsprüfer). Die Übertragung der eigenständigen Fachleistung des Verantwortlichen auf den Auftragsverarbeiter ist ausgeschlossen und nicht Gegenstand des Softwarevertrages.

Unbeschadet der durch weitere Vereinbarung abgeschlossenen Verschwiegenheitsverpflichtung des Auftragsverarbeiters als mitwirkende Person (i.S.d. § 203 Absatz 4 StGB) schließen die Vertragsparteien vorliegend eine Vereinbarung zur Auftragsverarbeitung wie folgt ab.

Inhaltsverzeichnis

Seite

1 Abkürzungen und Begriffsbestimmungen

In dieser Vereinbarung zur Auftragsverarbeitung gelten folgende Abkürzungen und Begriffsbestimmungen:

VFD:	Abkürzung für Verfahrensdokumentation.
Software:	Die Software *verfahrensdokumentation.pro* von smartcon, die Kunden internetbasiert als Software-as-a-Service zur Erstellung von VFD entgeltlich zur Verfügung gestellt wird.
Software-Hauptzweck:	Die Software dient der Erstellung, Speicherung und Aktualisierung von VFD.
Beraterkunde:	Kunden von smartcon, die als Berater (insbesondere als Steuerberater) von Unternehmen (primär) die Software zur Erstellung und Aktualisierung von VFD ihrer Mandanten und (sekundär) zur Erstellung der eigenen VFD nutzen.
Mandantennutzer:	Mandanten von Beraterkunden, deren VFD durch den Beraterkunden erstellt wird und die einen freigeschalteten Zugriff auf die Software haben.
Unternehmerkunde:	Kunden von smartcon, die als Unternehmen die Software *verfahrensdokumentation.pro* zur Erstellung und Aktualisierung ihrer eigenen VFD nutzen.
Softwarekunde:	Zusammenfassende Bezeichnung von Unternehmer- und Beraterkunden.
Softwarenutzer:	Kunden, Mandantennutzer als auch alle weiteren Personen (bspw. Mitarbeiter), die einen berechtigen Zugriff auf Software haben.
Daten:	Personenbezogene Daten (im Sinne des Art. 4 Ziff.1 DSGVO) von Kunden und Softwarenutzern.
SaaS-Vertrag:	Software-as-a-Servicevertrag, der zwischen smartcon und dem Softwarekunden bezüglich der entgeltlichen Nutzung der Software geschlossen wird.

2 Gegenstand räumliche Weite und Dauer der Auftragsverarbeitung

2.1 Gegenstand des Auftragsverarbeitung

Auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeitet smartcon als Betreiber der Software auftragsgemäß Daten für die Softwarekunden. Der Auftragsgegenstand ergibt sich aus dem zwischen den Parteien bestehenden **SaaS-Vertrag**, auf den verwiesen wird, sowie aus allen ergänzenden Vertragsvereinbarungen und -hinweisen. Eine nicht bestimmungsgemäße Erhebung, Verarbeitung oder Nutzung von Daten für fremde Zwecke ist ausgeschlossen, sofern keine diesbezügliche rechtliche Verpflichtung besteht.

2.2 Räumliche Weite der Datenverarbeitung

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des

Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2.3 Dauer der Vereinbarung und Sonderkündigungsrecht

Die Laufzeit dieses Auftragsverarbeitungsvertrages entspricht der Laufzeit des SaaS-Vertrages. Der Beraterkunde kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

3 Konkretisierung des Auftragsverhältnisses

3.1 Zweck der vorgesehenen Verarbeitung von Daten sowie Kategorien betroffener Personen

Smartcon stellt den Softwarekunden über das Internet die Software im Rahmen des SaaS-Vertrages und der ergänzenden Nutzungsbedingungen zur Erbringung des Softwarehauptzwecks zur Verfügung.

Smartcon verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, smartcon ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Smartcon verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

Der auftragsgemäße Hauptzweck umfasst die Verarbeitung personenbezogener Daten im Rahmen der fortzuentwickelnden Softwarebereitstellung (z. B. Softwarekundenbetreuung, Hilfe und Support, Analyse und Verbesserung des Dienstleistungsangebots des Auftragsverarbeiters).

3.2 Art der Verarbeitung (Art. 4 Nr. 2 DS-GVO)

Die regelmäßige Verarbeitung besteht im Erheben, Erfassen, Organisieren, Ordnen, Speichern, Bereitstellen sowie dem Einschränken und Löschen von Daten.

3.3 Art der vorgesehenen Verarbeitung von Daten sowie Kategorien betroffener Personen

Im Rahmen der Softwarenutzung und -bereitstellung werden Leistungen zur Datenverarbeitung sowie andere Dienstleistungen und Nebenleistungen ausgeführt. Der Auftragsverarbeiter erhält hierbei Zugriff auf die bei der Benutzung der in der vertragsgegenständlichen Software gespeicherten personenbezogenen Daten.

Aufgrund der durch die GoBD gebotenen revisionssicheren Speicherung der festgeschriebenen Verfahrensdokumentationen wird eine Protokollierung der Bearbeiter und Bearbeitungsstände als Nebenfunktion der Software *verfahrensdokumentation.pro* durchgeführt.

Folgende Datenkategorien können vom Verantwortlichen durch direkte Eingabe oder durch Hochladen in die Software *verfahrensdokumentation.pro* verarbeitet werden:

Angaben zum Verantwortlichen:

Stammdaten zum Beratungsunternehmen mit Stammdaten des Inhabers / der Gesellschafter / der Geschäftsführer, wie Name, Vorname und Anschrift, berufliche Qualifikationen, E-Mail-Adressen, Telefonnummern, Mobilfunknummern, Bankverbindung, Bestelldaten, Rechnungsdaten, Daten zum Zahlungsverhalten, Steuernummer / UST-ID Nr., Ansprechpartner, Sicherheitsfrage für Passwortverlust,

Zeitstempel und IP-Adresse des letzten Logins, durchgeführte Aktionen innerhalb von der Software *verfahrensdokumentation.pro.*

Angaben zu Erfüllungsgehilfen des Verantwortlichen:

Stammdaten der Erfüllungsgehilfen (insbesondere Mitarbeiter) des Verantwortlichen, wie Name und Anschrift von Mitarbeitern, E-Mail-Adressen, Telefonnummern, Mobilfunknummern, berufliche Qualifikationen, berufliche Funktion im Unternehmen des Verantwortlichen.

Angaben zu Mandanten des Verantwortlichen:

Stammdaten zu Mandanten des Verantwortlichen durch Stammdaten des Inhabers / der Gesellschafter / der Geschäftsführer, wie Name, Vorname und Anschrift, berufliche Ausbildung, E-Mail-Adresse, Telefonnummer, Mobilfunknummer, Zeitstempel und IP-Adresse des letzten Logins, durchgeführte Aktionen innerhalb von *verfahrensdokumentation.pro,* sowie Daten die im Rahmen der Softwarenutzung die unternehmerischen Verfahrensabläufe beim Mandanten erfasst werden.

Angaben zu Erfüllungsgehilfen des Mandanten:

Stammdaten der Erfüllungsgehilfen (insbesondere Mitarbeiter) des Mandanten, wie Name und Anschrift von Mitarbeitern, E-Mail-Adressen, Telefonnummern, Mobilfunknummern, berufliche Qualifikationen, berufliche Funktion im Unternehmen des Mandanten, Zeitstempel und IP-Adresse des letzten Logins, durchgeführte Aktionen innerhalb von der Software *verfahrensdokumentation.pro.*

Alle Kernfunktionen der Software *verfahrensdokumentation.pro* werden ausschließlich in Deutschland entwickelt und gehostet.

Jede Verlagerung einer Datenverarbeitung in ein Drittland außerhalb der EU/EWR bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in den USA wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO).

3.4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Ansprechpartner und Mitarbeiter des Verantwortlichen
- Ansprechpartner und Mitarbeiter bei Mandanten des Verantwortlichen
- Mitbenutzer (User), denen durch den Verantwortlichen insbesondere zur Freigabe von Verfahrensdokumentationen der Zugriff auf die Software *verfahrensdokumentation.pro* freigeschaltet wird, z.B. der Geschäftsführer des Mandanten des Verantwortlichen

4 Technische und organisatorische Maßnahmen

4.1 Einsatz von Rechenzentren und sonstigen Unterauftragsverarbeiter

Der Auftragsverarbeiter verpflichtet externe Software-Entwickler, externe Rechenzentren sowie sonstige Unterauftragsverarbeiter, die innerbetriebliche Organisation so zu gestalten, dass es den besonderen Anforderungen des Datenschutzes gerecht wird. Insbesondere findet die Datenverarbeitung auf Datenverarbeitungsanlagen statt, für die das Rechenzentrum oder der sonstige Unterauftragsverarbeiter alle technischen und organisatorischen gebotenen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Die Unterauftragsverarbeiter sind der **Anlage 2** zu entnehmen.

4.2 Maßnahmen zur Datensicherheit

Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten in **Anlage 1**).

4.3 Anpassung der Maßnahmen zur Datensicherheit

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.

5 Berichtigung, Einschränkung und Löschung von Daten

Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Eine datenschutzrechtlich unbedenkliche Einschränkung der Datenverarbeitung des Verantwortlichen durch den Auftragsverarbeiter aus berechtigtem Interesse und auf vertraglicher Grundlage bleibt unberührt. Soweit eine betroffene Person sich bezüglich der Datenverarbeitung unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Der Auftragsverarbeiter wird die Daten des Verantwortlichen nach dem Ende des SaaS-Vertrages wie folgt behandeln:

a. Die Daten des Beraterprofils, der angelegten Mandantenprofile und der gespeicherten Verfahrensdokumentations-Daten werden datenschutzkonform gelöscht. Daten, die der Auftragsverarbeiter aufgrund gesetzlicher Verpflichtungen (insbesondere handels- und steuerrechtliche Pflichten in Bezug auf Rechnungsdaten etc.) aufzubewahren hat, sind hiervon ausgenommen.

b. Der Verantwortliche kann jederzeit die vollständige datenschutzkonforme Löschung verlangen (Self-Service).

c. Der Verantwortliche kann jederzeit alle Daten in PDF-Format sowie ggf. in anderen gängigen Datenaustauschformaten exportieren.

Darüber hinaus sind zusätzliche Löschkonzepte, das Recht auf Vergessenwerden, die Berichtigung und Auskunft vom Verantwortlichen sicherzustellen.

6 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a. Der Auftragsverarbeiter sichert zu, dass er – sofern er zur Bestellung eines Datenschutzbeauftragten gesetzlich verpflichtet ist - einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt, dem die erforderliche Zeit zur Erledigung seiner Aufgaben gewährt wird. Eine vertragliche Pflicht zur Bestellung eines Datenschutzbeauftragten besteht nicht.

b. Zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO setzt der Auftragsverarbeiter bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 1).

d. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e. Der Verantwortliche informiert unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.

f. Soweit der Verantwortliche seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften im Rahmen der bestehenden Vertragspflichten zu unterstützen.

g. Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

7 Unterauftragsverhältnisse

Sofern der Auftragsverarbeiter Dritte im Rahmen von Unterauftragsverhältnissen einsetzt, gilt folgendes:

a. Als Unterauftragsverhältnisse im Sinne dieses Vertrags sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

b. Die Auslagerung auf Unterauftragsverarbeiter oder der Wechsel der bestehenden genehmigten Unterauftragsverarbeiter sind zulässig, soweit der Auftragsverarbeiter eine solchen Einschaltung von Unterauftragsverarbeitern dem Verantwortliche eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird. Im Falle des Einspruchs des Verantwortlichen steht dem Auftragsverarbeiter ein außerordentliches Kündigungsrecht sowohl

hinsichtlich dieser Vereinbarung als auch bezüglich der Leistungsvereinbarung (insbesondere des SaaS-Vertrages) zu.

c. Der Verantwortliche stimmt der Beauftragung der in der Anlage 2 vor Beginn der Verarbeitung mitgeteilten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

d. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

e. Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

8 Kontrollrechte des Verantwortlichen

a. Der Verantwortliche hat nach Vorankündigung das Recht, die Einhaltung der über die datenschutzrechtlichen Prozesse und der vertraglichen Vereinbarung durch den Auftragsverarbeiter oder das externe Rechenzentrum/den Unterauftragsverarbeiter zu kontrollieren. Dies kann entweder durch die Einholung von Auskünften oder die Vorlage von aktuellen Testaten, Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter) oder durch eine geeignete Zertifizierung mittels IT-Sicherheits- oder Datenschutzaudit erfolgen. Der Verantwortliche darf keinen Wettbewerber des Auftragsverarbeiters mit der Kontrolle beauftragen. 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.

b. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

9 Mitteilung bei Verstößen des Auftragsverarbeiters

a. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

   - die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
   - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden;
   - die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
   - die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung;
   - die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde;

b. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine angemessene oder vertraglich festgelegte Vergütung beanspruchen.

10 Weisungsbefugnis und Weisungen des Verantwortlichen

a. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

b. Die weisungsberechtigten Personen des Verantwortlichen und die Weisungsempfänger beim Auftragsverarbeiter sind jeweils schriftlich zu benennen. Bei einem Wechsel oder einer längerfristigen Verhinderung einer weisungsberechtigten Person oder eines Weisungsempfängers ist dem Vertragspartner unverzüglich schriftlich der Nachfolger oder Vertreter mitzuteilen.

c. 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 den Verantwortlichen bestätigt oder geändert wird.

11 Löschung und Rückgabe von personenbezogenen Daten

a. Kopien oder Duplikate der Daten 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.

b. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung (SaaS-Vertrag) – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten 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.

c. 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.

12 Schlussbestimmungen

d. Änderungen und Ergänzungen dieser Vertragsregelung und all 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 Vertragsregelung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

e. Sollten einzelne Teile dieser Vertragsregelung unwirksam sein, so berührt dies die Wirksamkeit der Vertragsregelung im Übrigen nicht. An Stelle der unwirksamen Bestimmung soll eine Bestimmung vereinbart werden, die dem von den Partnern hiermit verfolgten wirtschaftlichen Zweck möglichst nahekommt. Entsprechendes gilt im Falle einer Regelungslücke.

f. Diese Vertragsregelung unterliegt ausschließlich dem formellen und materiellen Recht der Bundesrepublik Deutschland. Die Anwendung des internationalen Privatrechts sowie des einheitlichen UN-Kaufrechts (CISG) wird ausdrücklich ausgeschlossen.

g. Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO tritt mit Abschluss in Textform in Kraft. Dem Verantwortlichen wird hierzu bei Registrierung die Verarbeitungsvereinbarung in Textform bereitgestellt. Diese hat der Verantwortliche bei Anmeldung in der Software zur Registrierung zu bestätigen.

1 Anlage 1: Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Maßnahmen, die gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt ist:

Die Hauptzugänge zu den Räumlichkeiten des Auftragsverarbeiters sind durch eine Schließanlage gegen unbefugte Zutritte gesichert. Es erfolgt eine kontrollierte und dokumentierte Schlüsselvergabe.
Der Zutritt zu den Räumlichkeiten mit Datenverarbeitungsanlagen findet ausschließlich in Begleitung eines Mitarbeiters statt.
Ein physischer Server ist vor Ort nicht vorhanden, die Datenverarbeitung findet über externe Rechenzentren mit hohem Sicherheitsstandard statt.

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Die Regelung des Zugangs zu den Datenverarbeitungssystemen erfolgt über ein Benutzer- und Berechtigungskonzept.
Der Zugang zu allen Systemen ist durch eine Anmeldung mittels Benutzerkennungen und individueller Passwörter gesichert. Es existiert eine Passwortrichtlinie mit festen Komplexitätsvorgaben und einem festen Änderungsrhythmus.
Das Netzwerk wird über eine Firewall und Virenscanner gesichert.
Die Mitarbeiter des Auftragsverarbeiters sind auf das Datengeheimnis und das Fernmeldegeheimnis sowie gegebenenfalls auf andere relevante Verschwiegenheitstatbestände verpflichtet.

1.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

Nur autorisierte Personen haben Zugriff auf die Systeme des Auftragsverarbeiters.
Das Berechtigungskonzept basiert auf dem „Need-to-Know-Prinzip“, d. h. es wird nur so viel Zugriff auf Daten eingeräumt, wie für den Zweck der Verarbeitung und die Aufgabenerfüllung unbedingt erforderlich ist.
Die Zugriffsberechtigungen werden den jeweiligen Funktionen der Mitarbeiter entsprechend vergeben und kontrolliert.
Die Maßnahmen der Zugriffskontrolle werden regelmäßig überprüft.

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit;

Der Auftragsverarbeiter arbeitet grundsätzlich mit IT-Systemen, die eine getrennte Verarbeitung von Daten im Sinne der Trennungskontrolle gewährleisten.

1.5 Pseudonymisierung

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.

Soweit möglich und im Einzelfall erforderlich wird das Gebot der Pseudonymisierung umgesetzt.

2 Anlage 1: Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Der Zugriff auf Server von extern erfolgt über den Stand der Technik entsprechend gesicherte verschlüsselte Verbindungen (z. B. VPN-Verbindungen). Es haben nur autorisierte Personen Zugriff auf die Systeme.
Soweit Daten zu beauftragten Partnern übertragen werden, sind diese Datenübertragungskanäle immer TLS verschlüsselt. Wo dies technisch möglich ist, kommen VPN-Verbindungen zum Einsatz.
Datenträger, die sensible Informationen (bspw. personenbezogene Daten, Betriebs – und Geschäftsgeheimnisse) enthalten, werden datenschutzkonform durch einen Entsorgungsdienstleister vernichtet.
Sofern ein Transport von Datenträgern erforderlich ist, erfolgt dieser gesichert.

2.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Die Eingabekontrolle wird durch Verfahrens- und Arbeitsanweisungen festgelegt. Zugriffe werden in systemspezifischen Logdateien protokolliert und bei Bedarf ausgewertet. Die Zugriffsberechtigung auf diese Logdateien ist streng reglementiert.

3 Anlage 1: Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Die Verfügbarkeitskontrolle wird beim Auftragnehmer durch folgende Maßnahmen sichergestellt:

- Backup- / Recoveryverfahren
- Es gibt ein dediziertes Konzept zur Rekonstruktion der Datenbestände und zudem eine regelmäßige Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können (Datenintegrität der Backups)
- Das Notfallkonzept wird regelmäßig überprüft und aktualisiert
- Mitarbeiter werden in regelmäßigen Abständen auf dieses Notfallkonzept geschult.
- Backups und Sicherungskopien sind über mehrere redundante Serversysteme und Rechenzentrumsstandorte verteilt
- Es werden Firewalls eingesetzt
- Sicherheitsrelevante Updates werden unverzüglich eingespielt
- Eine unterbrechungsfreie Stromversorgung (USV) in dem beauftragten Rechenzentrum ist sichergestellt
- Es gibt klare Meldewege sowie Brandschutzeinrichtungen

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Maßnahmen, die eine zeitnahe und vollständige Wiederherstellung von Daten sicherstellt;

- Mehrfach-redundante Auslegung von Serversystemen und Datenbanken
- Backups werden regelmäßig auf Wiedereinspielbarkeit geprüft
- Es gibt regelmäßige Notfallübungen, in denen Wiederherstellungsszenarien überprüft werden

4 Anlage 1: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management

Maßnahmen beim Auftragsverarbeiter, die gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Hinreichende Schulung der Mitarbeiter in Datenschutzangelegenheiten
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- Durchführung von Risiko- und Schwachstellenanalysen

4.2 Incident-Response-Management

Maßnahmen beim Auftragsverarbeiter, die gewährleisten, dass im Fall von Datenschutzverstößen ein Meldeprozess ausgelöst wird:

- Meldeprozess für Vertrags- und Datenschutzverletzungen gegenüber dem Kunden nach Art. 28 Abs. 3 Satz 3 sowie Art. 33 und Art. 34 DS-GVO), soweit erforderlich
- Etwaige Unterstützung für Kunden im Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Aufsichtsbehörden (Art. 33 DS-GVO)

4.3 Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

- Gewährleistung der Datenverarbeitung entsprechend der Weisung des Kunden durch enge Abstimmung zwischen Auftragsverarbeiter und Kunden
- Subunternehmen nur mit schriftlichen Datenschutzvereinbarungen nach Art. 28 DS-GVO
- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Kunden
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Formalisiertes Auftragsmanagement
- Verfahren zur Auswahl des Dienstleisters

Anlage 2: Auflistung der Unterauftragsverarbeiter

Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma	Anschrift	Leistung	Rechenzentren
Softwareentwicklung, Softwarehosting und Softwarespeicherung			
Divinci GmbH	Euerbacher Str. 2, 97424 Schweinfurt	Softwarebetreuung und -wartung, Programmierung zur Weiterentwicklung	Deutschland (EU)
Schuster & Walther IT-Business GmbH	Schwabacher Straße 3, 90439 Nürnberg	Hosting	Deutschland (EU)
DATEV eG	Paumgartnerstr. 6 –14, 90429 Nürnberg	Serverdienstleistung	Deutschland (EU)
Fakturierungs- und Zahlungssystem			
CHARGEBEE B.V.	Piet Heinkade 55, 1019 GM Amsterdam Niederlande	Fakturierungs- und Zahlungssystem	Europäischer Wirtschaftsraum