Vereinbarung über die Datenverarbeitung im Auftrag

STP Informationstechnologie GmbH
Brauerstraße 12
76135 Karlsruhe

nachfolgend „Auftragsverarbeiter“ nachfolgend „Verantwortlicher“

gemeinsam nachfolgend „Vertragspartner“

schließen folgende Vereinbarung:

1 Gegenstand der Vereinbarung

Der Verantwortliche steht mit dem Auftragsverarbeiter in einer kontinuierlichen Geschäftsbeziehung. In diesem Zuge verarbeitet der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen i. S. v. Art. 4 Nr. 1 DSGVO zur Erfüllung aktuell bestehender und künftig beschlossener Verträge über die Nutzung der Software des Auftragsverarbeiters als auch Dienstleistungen. In diesem Sinne wird das o. g. Unternehmen Auftragsverarbeiter im Sinne des Art. 28 DSGVO und § 62 BDSG in der ab 25.05.2018 gültigen Fassung.

1.1 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 Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG bzw. Art. 44 ff. DSGVO erfüllt sind.

1.2 Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags, Umfang und Art der Verarbeitung i. S. v. Art. 4 Abs. 2 DSGVO sowie die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt 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 Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Zweck der Datenverarbeitung ist die Ermöglichung der Leistungserbringung gemäß des Vertrags.

1.3 Art der von der Auftragsverarbeitung betroffenen personenbezogenen Daten i. S. v. Art. 4 Nr. 1 DSGVO:

- Personenstammdaten
- Kennnummern
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Bankdaten
- Online-Daten (z.B. IP-Adressen)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Mandats- und Verfahrensdaten
- Gläubigerinformationen und –bankdaten
- Statistikdaten zu Insolvenzverfahren

1.4 Kategorien betroffener Personen i. S. v. Art. 4 Nr. 1 DSGVO:

- Kunden
- Mandanten
- Interessenten
- Beschäftigte
- Lieferanten
- Beteiligte an einem Insolvenzverfahren
- Verwalter von Insolvenzverfahren

1.5 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen.

2 Rechte und Pflichten des Verantwortlichen

2.1 Der Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist für die Einhaltung der in Art. 5 Abs. 1 DSGVO normierten Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich. Er muss die Einhaltung dieser Grundsätze nachweisen können, Art. 5 Abs. 2 DSGVO. Er ist für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO und die Wahrung der Rechte der Betroffenen im Sinne von Art. Art. 12 bis 22 DSGVO verantwortlich. Dem Verantwortlichen obliegt es somit, die Rechtmäßigkeit der von ihm verantworteten Verarbeitungen personenbezogener Daten zu gewährleisten.

2.2 Der Auftragsverarbeiter darf personenbezogene Daten des Verantwortlichen nur zum Zwecke der Erbringung der Leistungen des Vertrages und nach Weisung des Verantwortlichen verarbeiten. Der Verantwortliche hat ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Verarbeitung personenbezogener Daten.

2.3 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des für die Verarbeitung Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

2.4 Weisungen des Verantwortlichen

a) Weisungen vom Verantwortlichen sind schriftlich oder per E-Mail zu erteilen. Alle Weisungen sollen sowohl vom Verantwortlichenals auch vom Auftragsverarbeiter zusammen mit dieser Vereinbarung so aufbewahrt werden, sodass alle maßgeblichen Regelungen jederzeit verfügbar sind. Der Auftragsverarbeiter ist berechtigt, die Durchführung einer mündlich erteilten Weisung solange auszusetzen, bis sie durch den Verantwortlichen schriftlich bestätigt wird.
b) Weisungsberechtigte Personen vom Verantwortlichen werden im Laufe der Inbetriebnahme festgelegt und an den Auftragsverarbeiter schriftlich kommuniziert.
c) Weisungsempfänger beim Auftragsverarbeiter werden im Laufe der Inbetriebnahme festgelegt und an den Verantwortlichen schriftlich kommuniziert.
d) Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich (E-Mail reicht aus) der Nachfolger oder der Vertreter mitzuteilen. Falls Weisungen die unter Ziff. 1 dieses Auftrags getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.

3 Rechte und Pflichten des Auftragsverarbeiters

3.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich nach den Weisungen des Verantwortlichen und für die erforderlichen auftragsbezogenen Tätigkeiten im Rahmen der getroffenen Vereinbarungen. Eine darüberhinausgehende Verarbeitung führt der Auftragsverarbeiter nur dann durch, wenn eine entsprechend Weisung des Verantwortlichen vorliegt. Der Auftragsverarbeiter verpflichtet sich, sich nur insoweit Kenntnis von personenbezogenen Daten des Verantwortlichen und fremden Geheimnissen zu verschaffen, als dies zur Auftragserfüllung erforderlich ist.

3.2 Der Auftragsverarbeiter bewahrt das Datenmaterial nicht länger auf, als es der Verantwortliche bestimmt. Gesetzliche Aufbewahrungsfristen bleiben unberührt.

3.3 Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen das Datengeheimnis zu wahren. Er bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind.

3.4 Der Auftragsverarbeiter verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Verantwortlichen obliegen. Er verpflichtet sich zur Verschwiegenheit über die vom Verantwortlichen überlassenen Daten und Informationen. Der Auftragsverarbeiter ist über die strafrechtlichen Folgen einer Pflichtverletzung belehrt.

3.5 Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes und der Geheimhaltung vertraut macht und sie auf das Datenschutzgeheimnis und die Vertraulichkeit schriftlich verpflichtet, Art. 28 Abs. 3 S. 2 lit. B und Art. 29 DSGVO.Der Auftragsverarbeiter überwacht die Einhaltung der datenschutz- und geheimhaltungsrechtlichen Vorschriften.

3.6 Der Auftragsverarbeiter wird i.S.v. Art. 32 DSGVO unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes und den rechtlichen Vorgaben entsprechendes Datenschutzniveau zu gewährleisten, Art. 28 DSGVO. Die konkreten Maßnahmen sind in Anhang 1 „Technische und organisatorische Schutzmaßnahmen (TOM)“ beschrieben. 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. Der Verantwortliche hat mit Blick auf die Schutzzwecke der für ihn im Auftrag verarbeiteten Daten das Datenschutzkonzept vor Vertragsschluss geprüft und als ausreichend bewertet.

3.7 Der Auftragsverarbeiter berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Verantwortliche dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragsverarbeiter auf Grund einer Einzelbeauftragung durch den Verantwortlichen, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Verantwortlichen zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

3.8 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Verantwortlichen entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Der Auftragsverarbeiter bestätigt dem Verantwortlichen die nach Maßgabe des Vertrages erfolgte Löschung der Daten. Hiervon ausgenommen sind Daten, für eine gesetzliche oder vertragliche Aufbewahrungsfrist besteht, sowie Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Verantwortliche.

3.9 Unabhängig von sonstigen Regelungen zur Löschung erfolgt die Löschung der Daten in den Sicherungssystemen und -dateien („Backups“) entsprechend dem regulären Turnus der Löschung dieser Backups.

3.10 Der Auftragsverarbeiter unterstützt – soweit erforderlich – den Verantwortlichen in angemessenem Umfang bei Anfragen und Kontrollen gemäß Ziff. 3.14 und Ziff. 4. Der Verantwortliche hat den Auftragsverarbeiter für seinen Aufwand im Rahmen dieser Unterstützung auf Stundenbasis gemäß der jeweils gültigen Preisliste des Auftragsverarbeiters zu entschädigen.

3.11 Der Auftragsverarbeiter wird den Verantwortlichen für dessen Datenschutz-Folgenabschätzung angemessen unterstützen.

3.12 Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind schriftlich mit dem Verantwortlichen abzustimmen.

3.13 Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, 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.

3.14 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, wird ihn der Auftragsverarbeiter nach besten Kräften unterstützen.

3.15 Der Auftragsverarbeiter hat für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau zu gewährleisten. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Es werden die erforderlichen Maßnahmen zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall und die rasche Wiederherstellung des Systems ergriffen (Art. 32 Abs. 1 lit. c DSGVO).

4 Anfragen Betroffener

4.1 Ist der Verantwortliche auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson oder einer Behörde verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, wird der Auftragsverarbeiter den Verantwortlichen dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Verantwortliche den Auftragsverarbeiter hierzu schriftlich oder in Textform aufgefordert hat und der Verantwortliche dem Auftragsverarbeiter die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragsverarbeiter wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Verantwortlichen verweisen.

4.2 Wendet sich ein Betroffener mit Forderungen zur Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) oder Sperrung bzw. Einschränkung der Verarbeitung (Art. 18 DSGVO) an den Auftragsverarbeiter, wird der Auftragsverarbeiter den Betroffenen an den Verantwortlichen verweisen.

5 Meldung von Störungen und Hinweispflichten des Auftragsverarbeiters

5.1 Der Auftragsverarbeiter überprüft in regelmäßigen Abständen die Einhaltung der Vorgaben dieser Vereinbarung, insbesondere der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Datensicherheit in Anhang 1 zu dieser Vereinbarung. Der Auftragsverarbeiter teilt dem Verantwortlichen Störungen bei der Auftragserledigung und Verletzungen des Datenschutzes, insbesondere der Datensicherheit, unverzüglich gemäß Art. 33 Abs. 2 DSGVO mit.

5.2 Stellt der Auftragsverarbeiter bei der Prüfung der Ergebnisse Unregelmäßigkeiten oder Fehler fest, informiert er den Verantwortlichen hierüber unverzüglich.

5.3 Falls der Auftragsverarbeiter der Ansicht ist, dass eine Weisung des Verantwortlichen gegen Datenschutzvorschriften verstößt, weist er den Verantwortlichen darauf hin. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Der Auftragsverarbeiter ist berechtigt (aber nicht verpflichtet), die Ausführung der Weisung zu unterlassen, bis die Weisung durch den Verantwortlichen schriftlich oder per Telefax bestätigt worden ist.

6 Kontrollrechte des Verantwortlichen

6.1 Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche jederzeit nach Vorankündigung mit einer angemessenen Frist mit dem Auftragsverarbeiter zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufes berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen

Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme (Art. 28 DSGVO)..

6.2 Zur Durchführung der Kontrolle muss der Auftragsverarbeiter nur eine solche Person zulassen, die besonders zur Geheimhaltung, insbesondere in Bezug auf Informationen über den Betrieb des Auftragsverarbeiters, dessen Ausstattung, Geschäftsgeheimnisse des Auftragsverarbeiters und Sicherheitsmaßnahmen, verpflichtet ist. Wird die Kontrolle nicht durch eine dem Auftragsverarbeiter diesbezüglich bereits bekannte Person durchgeführt, muss diese mindestens 7 Werktage vor Durchführung der Kontrolle ihre Legitimation durch den Verantwortlichen schriftlich oder per Telefax nachweisen.

6.3 Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn der Verantwortliche bei solchen Prüfungen oder in sonstiger Weise Fehler oder Unregelmäßigkeiten feststellt.

6.4 Sonstige vertragliche oder gesetzliche Kontrollrechte des Verantwortlichen bleiben unberührt.

7 Einsatz von Subunternehmen

7.1 Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in dem Anhang 2 aufgeführten Unternehmen als Subunternehmer für Teilleistungen für den Auftragsverarbeiter tätig und können in diesem Zusammenhang auch Zugriff auf die personenbezogenen Daten des Verantwortlichen haben. Für diese Subunternehmer gilt die Einwilligung für das Tätigwerden als erteilt.

7.2 Die Beauftragung von Subunternehmen nach Vertragsabschluss durch den Auftragsverarbeiter ist durch den Verantwortlichen zustimmungspflichtig. Der Auftragsverarbeiter stellt beim Verantwortlichen in Schriftform eine Anfrage zur Freigabe des Subunternehmens. Sollte sich der Verantwortliche nicht innerhalb von 2 Wochen in Schriftform zu der Freigabe äußern oder der Zustimmung aus einem wichtigen Grund widersprechen, so gilt die Zustimmung zum Subunternehmen als erteilt.

7.3 Erteilt der Auftragsverarbeiter Aufträge an Subunternehmer, so obliegt es dem Auftragsverarbeiter, seine Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Der Auftragsverarbeiter verpflichtet sich, die eingeschalteten Subunternehmen in Textform zur Verschwiegenheit und Vertraulichkeit hinsichtlich der vom Verantwortlichenüberlassenen Geheimnisse zu verpflichten. Eine etwaige Prüfung durch den Verantwortlichen beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragsverarbeiter. Durch schriftliche Aufforderung ist der Verantwortlichen berechtigt, vom Auftragsverarbeiter Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

7.4 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragsverarbeiter Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen, IT-Hosting oder Wartung. Der Auftragsverarbeiter wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

8 Datenschutzbeauftragter

Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, entsprechend den gesetzlichen Bestimmungen bei der zuständigen Aufsichtsbehörde gemeldet ist und einen betrieblichen Datenschutzbeauftragten entsprechend den gesetzlichen Vorgaben ausgewählt und bestellt hat. Der betriebliche Datenschutzbeauftragte des Auftragsverarbeiters nimmt seine Aufgaben nach den einschlägigen gesetzlichen Bestimmungen wahr. Datenschutzbeauftragter des Auftragsverarbeiters ist derzeit Daniel Kraft, Tel. +49 721 828 15-0.

9 Laufzeit und Kündigung

9.1 Diese Vereinbarung richtet sich nach den Laufzeiten und Kündigungsfristen des Vertrags zwischen den Parteien.

9.2 Mit Beendigung des Vertrages endet diese Vereinbarung automatisch, ohne dass es einer gesonderten Kündigung bedarf. Die Pflichten aus dieser Vereinbarung über die Auftragsverarbeitung gelten in jedem Fall auch nach einer Beendigung des Vertrages bis zur vollständigen Vernichtung oder Rückgabe aller im Zusammenhang mit dem Vertrag stehenden Daten durch den Auftragsverarbeiter.

9.3 Mit der Beendigung dieser Vereinbarung gemäß dieser Ziffer 9 endet die Tätigkeit des Auftragsverarbeiters für den Verantwortlichen.

10 Schlussbestimmungen

10.1 Wird eine vom Auftragsverarbeiter im Zusammenhang mit der Bereitstellung des Dienstes geschuldete Leistung aufgrund einer Weisung vom Verantwortlichen unmöglich gemacht oder wesentlich erschwert oder verlangt der Verantwortliche eine Löschung von Daten vor Ende des Auftrags, und ist der Auftragsverarbeiter aufgrund der Löschung ganz oder teilweise an der weiteren Leistungserbringung gehindert, so wird der Auftragsverarbeiter insoweit von seinen Leistungspflichten frei. Der Anspruch des Auftragsverarbeiters auf die vereinbarte Vergütung bleibt hiervon unberührt.

10.2 Erhöht sich aufgrund einer Weisung vom Verantwortlichen für den Auftragsverarbeiter der für die Leistungserbringung erforderliche Aufwand, kann der Auftragsverarbeiter eine entsprechende Anpassung der vereinbarten Vergütung verlangen. Der Auftragsverarbeiter hat den Verantwortlichen vor der zusätzlichen Leistungserbringung auf die zusätzlichen Kosten hinzuweisen und der Verantwortliche hat die Möglichkeit die Weisung zurückzunehmen, sodass keine zusätzlichen Kosten entstehen.

10.3 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. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Verantwortlichen als »verantwortlicher Stelle« im Sinne des BDSG bzw. der DSGVO liegen.

10.4 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

10.5 Es gilt deutsches Recht.

10.6 Die Anhänge sind Bestandteil dieses Vertrages:

- Anhang 1 Technische und organisatorische Schutzmaßnahmen
- Anhang 2 Zugelassene Subunternehmer

Ort, Datum	Ort, Datum
Unterschrift STP Informationstechnologie GmbH	Unterschrift Verantwortlicher

Anhang 1 zur Vereinbarung über die Auftragsverarbeitung

Technische und organisatorische Schutzmaßnahmen (TOM)

Der Auftragsverarbeiter trifft Maßnahmen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind zur:

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

a) Zutrittskontrolle

Zutrittskontrolle, also Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

Maßnahmen:

a) Der Zugang zu den Räumlichkeiten des Auftragsverarbeiters ohne besondere Aufsicht ist ausschließlich registrierten KeyCard-Besitzern gewährt.
b) Videoüberwachung der Zutrittspunkte des Gebäudes.
c) Der Zugang zum Serverraum ist nur der Geschäftsführung und den Administratoren gewährt.
d) Sämtliche Zugangstüren der Räumlichkeiten des Auftragsverarbeiters sind mit Keycardsystem ausgestattet. Die Keycardausgabe wird mit Anzahl und Art der Keycard, Name des Mitarbeiters, Datum sowie Unterschrift des Mitarbeiters durch die Personalabteilung dokumentiert.
e) Der Zutritt zu den Räumlichkeiten des Auftragsverarbeiters für firmenfremde Personen ist nur unter Aufsicht durch einen Mitarbeiter des Auftragsverarbeiters in den Räumlichkeiten des Auftragsverarbeiters zugelassen.

b) Zugangskontrolle

Zugangskontrolle, also zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen:

a) Nutzerkennungen an Workstations, Laptops, Servern etc., d.h. Nutzername und Passwort sind an den jeweiligen Nutzer gebunden und dürfen nicht weitergegeben werden. Bewegliche Datenverarbeitungs-systeme (Laptops) bzw. deren Datenträger (Festplatten) sind zusätzlich verschlüsselt.

c) Zugriffskontrolle

Zutrittskontrolle, also Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

Maßnahmen:

a) Der Zugang zu den Räumlichkeiten des Auftragsverarbeiters ohne besondere Aufsicht ist ausschließlich registrierten KeyCard-Besitzern gewährt.
b) Der Zugang zum Serverraum ist nur der Geschäftsführung und den Administratoren gewährt.

d) Trennungskontrolle

Das Ziel der Trennungskontrolle ist es zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten ebenfalls getrennt voneinander verarbeitet werden.

Maßnahmen:

a) Daten separater Aufträge werden grundsätzlich unabhängig voneinander verarbeitet und nicht zusammengeführt.
b) Daten des Verantwortlichen werden getrennt von Fremddaten abgelegt.

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten auf Datenträgern und Datenübertragungswegen gegen die Kenntnisnahme durch Dritte geschützt werden.

Maßnahmen:

a) Extern mobil genutzte Datenträger werden verschlüsselt (siehe Punkt 2 Zugangskontrolle). Daten werden an unterschiedlichen Stellen in der Programmstruktur gespeichert um alle Informationen nur über das Programm und die hinterlegten Zugriffsrechte, darzustellen.

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

a) Weitergabekontrolle

Weitergabekontrolle, also 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.

Maßnahmen:

a) Wege der Datenübertragung sind grundsätzlich vorab mit dem Verantwortlichen abzustimmen.

b) Soweit eine Speicherung von personenbezogenen Daten vor Ort auf ein mobiles Speichermedium zum Transport erfolgt, werden die Daten verschlüsselt und der Auftragsverarbeiter wird angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen.

c) Der Auftragsverarbeiter wird die, auf seinem Datenverarbeitungssystem und mobilen Speichermedien gespeicherten Daten nach Beendigung der Tätigkeit löschen. Die Datenlöschung wird vom Auftragsverarbeiter dokumentiert.

b) Eingabekontrolle

Eingabekontrolle, also zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

a) Es findet beim Auftragsverarbeiter keine generelle Protokollierung der einzelnen Arbeitsschritte statt.

b) Ein diesbezügliches Erfordernis ist dem Auftragsverarbeiter vor Auftragsdurchführung durch den Verantwortlichen schriftlich mitzuteilen.

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

a) Verfügbarkeitskontrolle

Verfügbarkeitskontrolle, also zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

a) Alle Rechner sind mit einem aktuellen Virenschutz ausgestattet. Das interne Netzwerk ist per Firewall vor externem Zugriff geschützt. Sofern erforderlich wird täglich ein komplettes Backup der Daten durchgeführt, sofern dies nicht systemseitig lediglich durch den Verantwortlichen erfüllt werden kann. Die Daten werden nach Beendigung des Auftrages gelöscht.

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

Zeitnahe und zügige Wiederherstellung des DV-Systems bei physischen oder technischen Zwischenfällen.

Maßnahmen:

a) Es existiert ein Notfallkonzept sowie dezentrale Sicherungsmedien, auf welche im Bedarfsfall kurzfristig zurückgegriffen werden kann.

b) Alle Rechner sind mit einem aktuellen Virenschutz ausgestattet. Das interne Netzwerk ist per Firewall vor externem Zugriff geschützt. Sofern erforderlich wird täglich ein komplettes Backup der Daten durchgeführt, sofern dies nicht systemseitig lediglich durch den Verantwortlichen erfüllt werden kann. Die Daten werden nach Beendigung des Auftrages gelöscht.

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

Bewertung und Evaluierung der Wirksamkeit technisch-organisatorischer Maßnahmen.

Maßnahmen:

Prüfung und Sicherstellung

Interne Audits, IT-Richtlinien und Datenschutzunterweisungen.

a) Incident-Response-Management

Cyber-Security-Prozess sowie Datenschutz-Prozesse bei potenziellen Datenschutzvorfällen.

b) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Datenschutz-Handouts und –Unterweisungen für neue Mitarbeiter.

c) Auftragskontrolle

a. Zwischen Auftragsverarbeiter und einem etwaigen Subunternehmer gibt es entsprechende Vereinbarungen die zumindest dem Sicherheitsniveau der Vereinbarungen zwischen Verantwortlichem und Auftragsverarbeiter entsprechen.
b. Sämtliche Mitarbeiter wurden zur Wahrung des Datengeheimnisses verpflichtet.

.

Anhang 2 zur Vereinbarung über die Auftragsverarbeitung

Zugelassene Subunternehmer sind:

1	STP Holding GmbH	Dienstleister		Brauerstraße 12 76135 Karlsruhe Deutschland
2	STP Solution GmbH	Technologie		Brauerstraße 12 76135 Karlsruhe Deutschland
3	Consiliari GmbH	Dienstleister		Brauerstraße 12 76135 Karlsruhe Deutschland
4	Ferber-Software GmbH	Technologie	3rd-Level-Support für LEXolution.FoMa	Konrad-Adenauer-Ring 1059557 Lippstadt Deutschland
5	gridscale GmbH	Technologie	Rechenzentrum für CLOUD-Server	Oskar-Jäger-Str 173 50825 Köln Deutschland
6	Salesforce Inc.	Technologie (Ticketsystem)	Cloud-Server sind in einem RZ in Frankfurt. Backup der Cloud ist in Frankreich.	Village 9 Floor 26 Salesforce Tower 110 Bishopsgate London, UK