Vorgehensweise
Auftragsverarbeitungsvertrag

Beiliegend finden Sie unseren Auftragsverarbeitungsvertrag. Diesen benötigen Sie, sobald Sie personenbezogene Daten an einen Dienstleister weitergeben. Gerne übersenden wir Ihnen diesen somit für Ihre Unterlagen zurück. Bitte gehen Sie dafür wie folgt vor:

1. **Ausfüllen:** Bitte füllen Sie die blauen Markierungen im Vertrag (Adresse am Dokumentenanfang sowie Ort und Datum beim Unterschriftenfeld) mit Ihren Daten aus
2. **Ausdrucken**: Bitte drucken Sie den Vertrag **zwei Mal** aus
3. **Unterzeichnen**: Bitte unterzeichnen Sie beide Exemplare des Vertrages als Auftraggeber
4. **Zusenden:** Bitte senden Sie uns beide Exemplare zurück an

   GTC TeleCommunication GmbH
   Bereich Datenschutz / -sicherheit
   Zimmermannstr. 15
   D-70182 Stuttgart

Wir übersenden Ihnen wenige Tage später ein von uns gegengezeichnetes Exemplar.

Auftragsverarbeitungsvertrag
Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO

zwischen:

-Verantwortlicher (Auftraggeber)-

und: GTC TeleCommunication GmbH
Zimmermannstraße 15
D-70182 Stuttgart
-Auftragsverarbeiter (Auftragsnehmer)-

als Anlage zum bestehenden Rahmenvertrag zwischen den Parteien

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, insbesondere die Anforderungen nach Artikel 28 EU-Datenschutzgrundverordnung („DSGVO"), die sich aus der im oben genannten Vertrag in seinen Einzelheiten beschriebenen Datenverarbeitung (insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung) ergeben. Sie findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte weitere Auftragsverarbeiter mit personenbezogenen Daten[1] des Verantwortlichen in Berührung kommen können, sofern dies in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einem Drittstaat erfolgt, für den ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt.

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Auftragsverarbeiter (Auftragnehmer) verarbeitet personenbezogene Daten von Kunden, Interessenten, Beschäftigten oder anderen Personengruppen des Verantwortlichen (Auftraggeber) ausschließlich im Auftrag und nach Weisung des Verantwortlichen. Der Zweck sowie die einzelnen Tätigkeiten und die Dauer des Auftrages werden im oben genannten Vertrag konkretisiert.

(2) Zur Wahrung der Rechte nach den datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie die Rechtmäßigkeit der Datenverarbeitung, ist der Verantwortliche verpflichtet.

[1] Artikel 4 Nr. 1 DSGVO: „Personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(3) Der Auftragsverarbeiter hat den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen. Möchte der Verantwortliche dem Antrag der betroffenen Person entsprechen, erfolgt eine entsprechende Weisung an den Auftragsverarbeiter.

§ 2 Umfang der Weisungsbefugnisse des Verantwortlichen gegenüber dem Auftragsverarbeiter

(1) Der Auftragsverarbeiter verarbeitet die vom Verantwortlichen überlassenen Daten ausschließlich im Rahmen der vertraglichen Bestimmungen und der Weisungen des Verantwortlichen. Gleiches gilt für das Erheben von Daten im Auftrag des Verantwortlichen. Änderungen im Verfahrensablauf beim Auftragsverarbeiter sind vorab mit dem Verantwortlichen abzustimmen und bedürfen der Schriftform. Die Verarbeitung der vom Verantwortlichen überlassenen oder für den Verantwortlichen erhobenen Daten zu eigenen Zwecken des Auftragsverarbeiters, ist in jedem Fall ausgeschlossen. 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.

(2) Sofern und soweit dies zur Erfüllung seiner Leistungsverpflichtung erforderlich ist, ist der Auftragsverarbeiter unter Einhaltung der Bestimmungen dieser Vereinbarung zur Durchführung aller erforderlichen Verarbeitungsschritte der vom Verantwortlichen überlassenen sowie der ggf. für ihn erhobenen Daten (z.B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Log-Files, Zwischendateien und Arbeitsbereichen etc.) berechtigt.

(3) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder eines Mitgliedsstaates der Europäischen Union verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen.

(4) Unbeschadet der Artikel 82, 83 und 84 DSGVO gilt ein Auftragsverarbeiter, der unter Verstoß gegen die DSGVO die Zwecke und Mittel der Verarbeitung bestimmt und damit insbesondere die Weisungen überschreitet, in Bezug auf diese Verarbeitung als Verantwortlicher

§ 3 Übersicht über Art und Zweck der vom Auftragsverarbeiter verarbeiteten Daten, Art der personenbezogenen Daten und Kategorien der betroffenen Personen gemäß der im Vertrag festgelegten Leistungsbeschreibung

(1) **Umfang**: wiederkehrend

(2) **Art der Verwendung der Daten**: Erfassung, Speicherung, Übermittlung, Löschung/Vernichtung, Sperrung, Nutzung von Daten.

(3) **Zweck:**

Die Daten werden zu den im oben genannten Vertrag beschriebenen Zwecken, das heißt mit den darin genannten Tätigkeiten verarbeitet.

(4) **Art der Daten/Betroffenenkreis**:

Interessentendaten bzw. Daten von Nichtkunden natürlicher Personen	☐
Interessentendaten bzw. Daten von Nichtkunden juristischer Personen	☐
Kundendaten natürlicher Personen	☐
Kundendaten juristischer Personen	☐
Beschäftigtendaten	☐
Sonstige (personenbezogene) Daten (z. B. Lieferantendaten)	☐

(5) **Besondere Arten personenbezogener Daten (Artikel 9 DSGVO)**:

Gesundheit/Sexualleben	☐
Gewerkschaftszugehörigkeit/Betriebsrat	☐
Religiöse/weltanschauliche Überzeugungen	☐
Politische Meinungen	☐
Rassische/ethnische Herkunft	☐
Genetische/biometrische Daten	☐
Gesichtsbilder zur eindeutigen Identifizierung	☐

§ 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter hat dafür zu sorgen und hinreichende Garantien im Sinne der DSGVO dafür zu bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
Der Auftragsverarbeiter sichert in seinem Verantwortungsbereich die dauerhafte Einhaltung der vereinbarten allgemeinen sowie technischen und organisatorischen Maßnahmen entsprechend Artikel 32 DSGVO zu.
Der Auftragsverarbeiter hat hierbei 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. Insbesondere wird der Auftragsverarbeiter seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (diesbzgl. Mindestanforderungen sind in **Anlage „Technisch-organisatorische Maßnahmen"** i.S.d. Artikel 32 DSGVO aufgeführt). Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Verantwortlichen vor Missbrauch und Verlust treffen, die den Anforderungen der DSGVO entsprechen.

(2) Der Auftragsverarbeiter sichert zu, dass er über die erforderliche Herrschaft über die Datenverarbeitungsanlagen verfügt, mit denen personenbezogene Daten des Verantwortlichen verarbeitet werden. Dies schließt etwaige Eigentums- oder Besitzrechte ein.

(3) Der Datenschutzbeauftragte des Auftragsverarbeiters berichtet dem Verantwortlichen unverzüglich bei Änderungen zu den getroffenen technischen und organisatorischen Sicherheitsmaßnahmen.

§ 5 Zulässigkeit der Begründung von Unterauftragsverhältnissen (weitere Auftragsverarbeiter) und Bedingungen für deren Einsatz

(1) Die Beauftragung eines weiteren Auftragsverarbeiters durch den Auftragsverarbeiter (Subunternehmer) zur Erfüllung einer Leistungsverpflichtung aus dem o.g. Vertrag, bedarf der vorherigen schriftlichen Zustimmung des Verantwortlichen.

(2) Eine allgemeine Vorabzustimmung zur Beauftragung weiterer Subunternehmers im Sinne des Artikel 28 Abs. 2 DSGVO erfolgt grundsätzlich nicht.
Sofern eine solche Zustimmung nach Satz 1 abweichend von dieser Vereinbarung dennoch ausdrücklich und schriftlich vereinbart wird, informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, rechtzeitig gegen derartige Änderungen Einspruch einzulegen. Zur Beurteilung, ob ein Einspruch durch den Verantwortlichen geltend gemacht wird, stellt der Auftragsverarbeiter dem Verantwortlichen aussagekräftige Informationen über den Subunternehmer zur Verfügung.

(3) Nicht der Zustimmung nach Absatz 1 unterliegen solche Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen zum Beispiel Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(4) Subunternehmer, deren Einsatz zur Durchführung des vereinbarten Auftrages als weiter beauftragte Auftragsverarbeiter bei Abschluss des oben genannten Vertrages nach Absatz 1 gebilligt sind, werden in der Anlage zu dieser Anlage benannt. Hierbei ist für jeden Subunternehmer der Leistungsort und die beauftragte Leistung zu beschreiben.

(5) Die Verarbeitung der Daten durch den nach Absatz 1 gebilligten Subunternehmer ist erst dann zulässig, wenn der Subunternehmer eine Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO unterzeichnet und die geeigneten Garantien nach Artikel 28 Abs. 1 DSGVO nachgewiesen hat.

(6) Der Auftragsverarbeiter hat sicherzustellen, dass der nach Absatz 1 gebilligte Subunternehmer in gleicher Weise wie er selbst vertraglich verpflichtet wird. Dies gilt insbesondere im Hinblick auf die Kontrollrechte des Verantwortlichen (§ 11) und die Informationspflichten (§ 12). Der Auftragsverarbeiter hat die Einhaltung der Pflichten regelmäßig zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren.

(7) Die Verarbeitung der personenbezogenen Daten durch den nach Absatz 1 gebilligten Subunternehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einem Drittstaat statt, für den ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt.
Jede Verarbeitung in anderen Ländern oder bei einer internationalen Organisation bedarf der vorherigen schriftlichen Zustimmung des Verantwortlichen.
Die Übermittlung in ein Drittland oder an eine internationale Organisation darf im Falle einer Zustimmung nur erfolgen, wenn die besonderen Voraussetzungen des Kapitel V der DSGVO erfüllt sind, sofern der Auftragsverarbeiter nicht durch das Recht der Europäischen Union oder eines Mitgliedsstaats der Europäischen Union, dem er unterliegt, hierzu verpflichtet ist. 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.

§ 6 Mandantenfähigkeit

Der Auftragsverarbeiter stellt sicher, dass die dem oben genannten Vertrag unterliegenden personenbezogenen Daten getrennt von anderen Mandaten verarbeitet werden. Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden. Dies setzt eine jederzeitige Trennung (physisch oder logisch) und wechselseitige Abschirmung der für die jeweiligen Verarbeitungszwecke und Mandanten verarbeiteten Datenbestände voraus.

§ 7 Datengeheimnis / Fernmeldegeheimnis

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die personenbezogenen Daten, zu denen sie Zugang haben ausschließlich auf Weisung verarbeiten, es sei denn, dass sie nach dem Recht der Europäischen Union oder dem Recht der Mitgliedsstaaten der Europäischen Union zur Verarbeitung verpflichtet sind.

(2) Die vom Auftragsverarbeiter eingesetzten Mitarbeiter und gegebenenfalls von ihm beauftragten Subunternehmer sind zur absoluten Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet. Informationen über den Kunden dürfen nur vom Verantwortlichen selbst oder vom Auftragsverarbeiter nach vorheriger schriftlicher Zustimmung des Verantwortlichen weitergegeben werden, wenn gesetzliche Bestimmungen dies gebieten oder der Kunde eingewilligt hat oder der Verantwortliche zur Erteilung einer Auskunft befugt ist.

(3) Die Verpflichtung dieser Personen auf die Wahrung der Vertraulichkeit nach Absatz 1 muss vor der erstmaligen Aufnahme ihrer Tätigkeit für den Verantwortlichen vorgenommen sein und ist dem Verantwortlichen auf Verlangen mittels unterschriebener Verpflichtungserklärung nachzuweisen. Sofern im oben genannten Vertrag keine abweichende Vereinbarung getroffen wurde, gilt die Verpflichtung zur Gewährleistung der Vertraulichkeit nach Absatz 1 über die Beendigung dieses Vertrages hinaus.

(4) Der Auftragsverarbeiter stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Verantwortlichen befassten Mitarbeiter und gegebenenfalls von ihm beauftragte Subunternehmer regelmäßig in den anwendbaren Datenschutzvorschriften geschult werden.

(5) Wirken Personen des Auftragsverarbeiters und gegebenenfalls von ihm beauftragte Subunternehmer am technischen Vorgang der Erbringung von Telekommunikationsdiensten für den Verantwortlichen mit, so erstreckt sich diese Sorgfaltspflicht auch auf das Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz oder einer entsprechenden anwendbaren gesetzlichen Bestimmung des betreffenden Rechtsraumes. Die Verpflichtung dieser Personen auf die Wahrung des Fernmeldegeheimnisses muss vor der erstmaligen Aufnahme der Tätigkeit für den Verantwortlichen vorgenommen sein und ist dem Verantwortlichen auf Verlangen mittels unterschriebenen Erklärungsformulars nachzuweisen.

(6) Auskünfte darf der Auftragsverarbeiter und gegebenenfalls der von ihm beauftragte Subunternehmer nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

§ 8 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter hat ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept, das den Anforderungen des Artikels 32 DSGVO genügt, zu erstellen. Auf Wunsch des Verantwortlichen stellt der Auftragsverarbeiter das Datenschutz- und Sicherheitskonzept zur dem Verantwortlichen Verfügung oder gewährt im erforderlichen Umfang Einblick in dieses Konzept.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen, die für den Inhalt des Verzeichnisses nach Artikel 30 Abs. 1 DSGVO wesentlichen Angaben zur Verarbeitung zusammenzustellen, wie zum Beispiel Zweck der Verarbeitung, Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger. Der Auftragsverarbeiter erstellt weiterhin ein Verzeichnis nach Artikel 30 Abs. 2 DSGVO. Dieses Verzeichnis muss alle Kategorien der von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung enthalten.

(3) Die Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einem Drittstaat statt, für den ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt.
Jede Verarbeitung in anderen Ländern oder bei einer internationalen Organisation bedarf der vorherigen schriftlichen Zustimmung des Verantwortlichen.
Die Übermittlung in ein Drittland oder an eine internationale Organisation darf im Falle einer Zustimmung nur erfolgen, wenn die besonderen Voraussetzungen des Kapitel V der DSGVO erfüllt sind, sofern der Auftragsverarbeiter nicht durch das Recht der Europäischen Union oder eines Mitgliedsstaats der Europäischen Union, dem er unterliegt, hierzu verpflichtet ist. 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

(4) Vom Verantwortlichen an den Auftragsverarbeiter überlassene Datenträger verbleiben im Eigentum des Verantwortlichen bzw. in dessen dauerhafter Verfügungsbefugnis. Der Auftragsverarbeiter übereignet dem Verantwortlichen zur Sicherung alle anderen Datenträger, auf denen sich Dateien befinden, die Daten des Verantwortlichen enthalten bzw. verschafft dem Verantwortlichen die dauerhafte Verfügungsbefugnis. Der Auftragsverarbeiter hat diese besonders zu kennzeichnen und sorgfältig zu verwahren, so dass sie Dritten und unberechtigten Personen nicht zugänglich sind.
Ist es dem Auftragsverarbeiter wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich diesen Pflichten nachzukommen, so treten an die Stelle der Rückgabe von Datenträgern die Bestimmungen zur Löschung oder Einschränkung nach § 14.

(5) Die Verarbeitung von personenbezogenen und sonstigen Daten des Verantwortlichen an Heimarbeitsplätzen und in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des Verantwortlichen im Einzelfall gestattet.
Sofern die Verarbeitung der Daten nach Satz 1 gebilligt ist, ist der Auftragsverarbeiter dafür verantwortlich, dass angemessene und geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
Der Auftragsverarbeiter ist zudem dafür verantwortlich, dass die erforderlichen Besichtigungs- und Kontrollrechte des Verantwortlichen nach § 11 uneingeschränkt gewährleistet bleiben. Der Zugang zur Privatwohnung durch den Verantwortlichen ist vorher mit dem Auftragsverarbeiter abzustimmen. Der Auftragsverarbeiter sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

Kann das Besichtigungs- und Kontrollrecht durch den Verantwortlichen nicht gewährleistet werden, so ist die Verarbeitung an Heimarbeitsplätzen und in Privatwohnungen untersagt.
Die Verarbeitung von personenbezogenen und sonstigen Daten des Verantwortlichen in öffentlich zugänglichen Räumen ist untersagt.

(6) Unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen, hat der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in den Artikel 32 bis 36 DSGVO genannten Pflichten zu unterstützen.

(7) Der Auftragsverarbeiter ist zur Einhaltung insbesondere der Artikel 10 sowie 24 bis 42 DSGVO verpflichtet, soweit sie für dieses Vertragsverhältnis von Relevanz sind. Auf Anfrage durch den Verantwortlichen stellt der Auftragsverarbeiter dem Verantwortlichen aussagekräftige Nachweise zur Erfüllung dieser Pflichten zur Verfügung, sofern diese für die vereinbarte Auftragsverarbeitung relevant sind.

§ 9 Datenschutzbeauftragter des Auftragsverarbeiters

(1) Der benannte Datenschutzbeauftragte des Auftragsverarbeiters ist dem Verantwortlichen mitzuteilen. Falls die Datenverarbeitung in Ländern erfolgt, in denen die Benennung eines Datenschutzbeauftragten nicht verbindlich ist oder kein Datenschutzbeauftragter benannt wurde, sind die Kontaktdaten der für die Einhaltung von Datenschutzvorschriften verantwortlichen Person dem Verantwortlichen mitzuteilen.

Der Datenschutzbeauftragte des Auftragsverarbeiters ist in § 19 benannt.

(2) Der Datenschutzbeauftragte bzw. die für die Einhaltung von Datenschutzvorschriften verantwortliche Person des Auftragsverarbeiters, hat seine Tätigkeit gemäß den Artikel 37 bis 39 DSGVO auszuüben. Er hat insbesondere auf die Einhaltung der anwendbaren Datenschutzvorschriften im Hinblick auf das Auftragsverhältnis hinzuwirken.

(3) Die Parteien informieren sich gegenseitig unverzüglich über einen Wechsel in der Person des Datenschutzbeauftragten bzw. der für die Einhaltung von Datenschutzvorschriften verantwortlichen Person.

§ 10 Rechte der betroffenen Personen

Sofern Rechte von durch die Datenverarbeitung betroffenen Personen beim Auftragsverarbeiter geltend gemacht werden ist der Verantwortliche für die Wahrung dieser Rechte verantwortlich.

§ 11 Kontrollrechte des Verantwortlichen; Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter räumt dem Verantwortlichen diejenigen Auskunfts-, Einsichts-, Zutritts-, Zugangs-, Zugriffs- und Kontrollrechte ein, die notwendig sind,

damit der Verantwortliche gemäß Artikel 28 Abs. 3h DSGVO die ordnungsgemäße Erbringung der Vertragsleistungen überwachen und prüfen kann, soweit sie die Verarbeitung der Daten des Verantwortlichen betreffen.
Der Verantwortliche kann sich nach Anmeldung zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten von der Einhaltung der in dieser Vereinbarung getroffenen Abreden überzeugen. Der Auftragsverarbeiter wird dem Verantwortlichen ermöglichen innerhalb von 3 Kalenderwochen die Prüfung in den Betriebsstätten des Auftragsverarbeiters zu beginnen.

(2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Prüfung erforderlich sind.

3) Im Hinblick auf die hiernach bestehenden Kontrollverpflichtungen vor Beginn der Datenverarbeitung und sodann 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 die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO nach. Als Nachweis kann der Auftragsverarbeiter auch aktuelle, aussagekräftige Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), Nachweise der Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO oder eine geeignete Zertifizierung gemäß Artikel 42 DSGVO vorlegen.
Das eigene Kontroll- und Überprüfungsrecht durch den Verantwortlichen bleibt hiervon unberührt.

§ 12 Informationspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen, bei Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen oder sonstigen Daten des Verantwortlichen oder bei Verletzung der im Vertrag zur Auftragsverarbeitung getroffenen Festlegungen.

(2) Es ist bekannt, dass nach Artikel 33 und 34 DSGVO für den Verantwortlichen Melde- und Benachrichtigungspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle gemäß Artikel 33 Abs. 2 DSGVO 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) 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 relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Verantwortlichen liegt.
Der Auftragsverarbeiter ist nicht befugt, jegliche Art von Rechten an den Daten des Verantwortlichen geltend zu machen. Dazu zählen zum Beispiel Eigentums-, Zurückbehaltungs- und Sicherungsrechte.

(4) Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragsverarbeiter das Ergebnis dem Verantwortlichen bekannt zu geben, soweit es die Verarbeitung der Daten des Verantwortlichen betrifft. Die im Prüfbericht feststellten Mängel wird der Auftragsverarbeiter unverzüglich abstellen und den Verantwortlichen darüber informieren.

(5) Dem Verantwortlichen werden durch den Auftragsverarbeiter die zusammenfassenden, relevanten Prüfberichte des Datenschutzbeauftragten des Auftragsverarbeiters zur Verfügung gestellt, soweit sie die Verarbeitung der Daten des Verantwortlichen betreffen. Die im Prüfbericht festgestellten Mängel wird der Auftragsverarbeiter unverzüglich abstellen und den Verantwortlichen darüber informieren.

(6) Die Absätze 1 bis 5 gelten entsprechend für Vorkommnisse bei Prozessen, die von Subunternehmern ausgeführt werden.

§ 13 Regelmäßige Prüfung des Angemessenheitsbeschlusses

(1) Erfolgt die Datenverarbeitung in einem Drittstaat, für den ein Angemessenheitsbeschluss der Europäischen Kommission im Sinne des Artikels 45 DSGVO vorliegt, so überprüfen der Verantwortliche und der Auftragsverarbeiter regelmäßig die Fortgeltung des Angemessenheitsbeschlusses[2].

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, sofern ihm bekannt wird, dass der Angemessenheitsbeschluss aufgehoben, geändert oder ausgesetzt wird bzw. wurde.

(3) Der Verantwortliche behält sich das Recht zur außerordentlichen Kündigung vor, falls die Wirkung des Angemessenheitsbeschlusses gemäß Bericht nach Artikel 45 Abs. 3 Satz 2 in Verbindung mit Artikel 45 Abs. 5 DSGVO aufgehoben, geändert oder ausgesetzt wird bzw. wurde.

§ 14 Rückgabe überlassener Auftragsmaterialien; Berichtigung, Löschung und Einschränkung von Daten durch den Auftragsverarbeiter

(1) Überlassene Dokumente, personenbezogene Daten und Datenträger sowie Kopien derselben sind grundsätzlich nach Beendigung des Auftrags nach Wahl des Verantwortlichen entweder durch den Auftragsverarbeiter zu löschen, einzuschränken, zurückzugeben oder zu vernichten, sofern nicht nach dem Recht der

[2] Eine Liste ist hier verfügbar:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Europäischen Union oder dem Recht der Mitgliedsstaaten der Europäischen Union eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
Der Verantwortliche kann auch vorher jederzeit die Löschung, Einschränkung, Herausgabe oder Vernichtung verlangen.

(2) Soweit Daten vom Auftragsverarbeiter berichtigt, gelöscht, eingeschränkt, herausgegeben oder vernichtet werden sollen, erfolgt dies ausschließlich auf Weisung des Verantwortlichen. Die Vorgänge sind mit Angabe von Datum und durchführender Person zu protokollieren. Die Protokolle sind dem Verantwortlichen auf Verlangen zur Verfügung zu stellen.

(3) Die physische Vernichtung von Dokumenten und Datenträgern hat – sofern keine andere Weisung vorliegt - mindestens nach DIN 66399 Sicherheitsstufe 3 oder in ihrer Entsprechung und Wirkung nach DIN EN 15713 zu erfolgen.

(4) Erfolgt eine Datenlöschung beim Auftragsverarbeiter, hat der Auftragsverarbeiter sämtliche löschbaren elektronischen Datenträger, die Daten des Verantwortlichen enthalten, datenschutzgerecht und nicht wieder herstellbar zu löschen. Daten in Datenbanksystemen sind so aus der logischen Struktur zu löschen, dass die Löschung nicht rückgängig gemacht werden kann. Der Auftragsverarbeiter ist verpflichtet, technisch oder organisatorisch sicherzustellen, dass die Daten auch tatsächlich gelöscht werden. Hierüber hat der dem Verantwortlichen einen Nachweis zu erbringen.

§ 15 Sonstige Verpflichtungen über das Vertragsende hinaus

(1) Dokumentationen, die dem Nachweis der ordnungsmäßigen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Verantwortlichen bei Vertragsende übergeben. Der Auftragsverarbeiter hat im Regressfall dem Verantwortlichem auch nach Vertragsende die noch vorhandenen Dokumentationen zur Führung des Entlastungsbeweises bei einer eventuellen Schadensersatzforderung wegen behaupteter unzulässiger oder unrichtiger Datenverarbeitung zu überlassen.

(2) Die Vertragspartner sind verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus, zeitlich unbegrenzt Stillschweigen über die ihnen im Zusammenhang mit dem Auftrag bekannt gewordenen Daten und Sachverhalte zu wahren.

§ 16 Haftung

(1) Für den Ersatz von Schäden und Mehraufwendungen, die dem Verantwortlichen wegen einer nach der DSGVO oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen Verarbeitung personenbezogener Daten im Rahmen des Auftragsverhältnisses entstehen, ist der Auftragsverarbeiter gegenüber dem Verantwortlichen verantwortlich. Unzulässig in diesem Sinne meint insbesondere die Verarbeitung, welche von den Weisungen des Verantwortlichen abweicht sowie die fehlerhafte Verarbeitung aufgrund von Prozessfehlern des Auftragsverarbeiters. Der Auftragsverarbeiter wird dem Verantwortlichen von eventuellen Ansprüchen Dritter in diesem Zusammenhang freistellen.

(2) Im Übrigen gelten bezüglich der Haftung die Haftungsregelungen aus dem oben genannten Vertrag. Sollten keine Haftungsregelungen im oben genannten Vertrag vereinbart worden sein, so gelten die gesetzlichen Bestimmungen zur Haftung.

§ 17 Sonstiges

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich gesonderter Weisungen, die diesen Auftrag im Einzelfall konkretisieren - 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 diese Formerfordernis.

(2) Es gilt die im oben genannten Vertrag vereinbarte Rechtswahl. Sofern dort keine Regelung vereinbart wurde, gilt das Recht der Bundesrepublik Deutschland.

§ 18 Unterschriften

Diese Anlage ist nur wirksam, sofern sie von den Vertragsparteien unterschrieben wurde.

§ 19 Datenschutzbeauftragte

Beim **Auftragnehmer** ist als Beauftragte für den Datenschutz (DSB) bestellt:
Name: Frau Simone Wankmüller

§ 20 Besonderer Hinweis

Soweit diese Vereinbarung auf Vorschriften aus der DSGVO verweist, die erst ab dem 25.05.2018 Ihre gesetzliche Geltung entfalten, vereinbaren die Parteien, dass die Inhalte der jeweiligen Vorschriften zwischen ihnen bereits vom Zeitpunkt des Abschlusses dieser Vereinbarung bis zum 25.05.2018 entsprechende Anwendung finden. Im vorgenannten Zeitraum ist diese Vereinbarung also umzusetzen, als ob die Regelungen der DSGVO bereits anzuwenden seien. Ab dem 25.05.2018 entfällt dieser § 20 ersatzlos.

_____
(Vorname Name in Klarschrift)

_____ _____
(Ort, Datum) (Unterschrift Verantwortlicher)

_____
(Vorname Name in Klarschrift)

_____ _____
(Ort, Datum) (Unterschrift Auftragsverarbeiter)

Anlage – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit

Zutrittskontrolle

Der Auftragnehmer sichert zu, durch folgende Maßnahmen Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle):

1) Zentraler Zugang nur über den Empfang… .....
2) Zutritt zu den Büroräumen erfolgt nur durch berechtigte Mitarbeiter bzw. in deren Begleitung .....
3) Schlüsselordnung mit Dokumentation sämtlicher Schlüssel-Inhaber.....
4) Separat verschlossener und gesicherter Server-Raum .....
5) Alarmanlagen-gesicherte Räume……. .....

Zugangskontrolle

Der Auftragnehmer sichert zu, durch folgende Maßnahmen zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle):

1) Zugangsberechtigungen nur für berechtigte Mitarbeiter .....
2) Zugangskontrollen, Anwesenheitsaufzeichnung .....
3) Passwortschutz mit entsprechenden Passwortvorgaben .....

Zugriffskontrolle

Der Auftragnehmer sichert zu, durch folgende Maßnahmen dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

1) Differenzierte Zugriffsrechte je nach Funktion und Mitarbeiter.....
2) Passwortkontrollen .....
3) Umfangreiche Protokollierung und regelmäßige Sichtung der Zugriffe .....

Trennungskontrolle

Der Auftragnehmer sichert zu, durch folgende Maßnahmen dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle):

1) Mandantenfähige Systeme……. .....
2) Umfangreiche Arbeitsanleitungen und Stellenbeschreibungen .....
3) Datenschutzbeauftragter .....

Pseudonymisierung
Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, es sei denn, es handelt es sich hierbei um auftragsbezogene Daten, bei denen eine Zuordnung für die ordnungsgemäße Abwicklung des Auftrages notwendig ist.

2. Integrität
Weitergabekontrolle
Der Auftragnehmer sichert zu, durch folgende Maßnahmen dafür Sorge zu tragen, dass dem Auftraggeber gesicherte Übertragungswege für die Datenübertragung personenbezogener Daten zur Verfügung stehen, bei deren Nutzung die Daten auch während der Übermittlung 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 (Weitergabekontrolle):

1) Standard-PC der Mitarbeiter ohne externe Speichermöglichkeit .....
2) Dokumentation der elektronischen Übermittlungen durch Logfiles .....
3) Lagerung von Datenträgern separat gesichert und dokumentiert .....

Eingabekontrolle
Der Auftragnehmer sichert zu, durch folgende Maßnahmen dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):

1) Festlegung konkreter Zuständigkeiten und Zugriffsrechte.....
2) Protokollierung der Dateneingabe .....

3. Verfügbarkeit und Belastbarkeit
Verfügbarkeitskontrolle
Der Auftragnehmer sichert zu, durch folgende Maßnahmen dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle):

1) Redundante Serverstrukturen .....
2) Umfangreiche und regelmäßige Datensicherungen.....
3) Notstromversorgung.....
4) Aufbewahrung der Datensicherungen in feuergeschütztem Bereich.....
5) Umfangreicher Virenschutz und Firewall.....

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die eingesetzten Verfahren werden in regelmäßigen Abständen überprüft, bewertet und evaluiert. Dies wird durch ein entsprechendes Datenschutz-Management sichergestellt.

Auftragskontrolle

Der Auftragnehmer sichert zu, durch folgende Maßnahmen dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):

1) Definition und Dokumentation der Abläufe und Zuständigkeiten.. .....
2) Umfangreiche Kontrolle während der manuellen Auftragsbearbeitung.....
3) Auftragsdatenverarbeitungsvertrag…. .....