

Bendel & Schrade GmbH

Vereinbarung zur Auftragsverarbeitung

zwischen

Unternehmen

Straße

Plz Ort

- nachfolgend "Auftraggeber" genannt -

und

Bendel & Schrade GmbH

Am Heselsberg 20

88416 Ochsenhausen

- nachfolgend „Auftragnehmer“ genannt -

- gemeinsam die „Parteien“ genannt -

Inhaltsverzeichnis

Präambel	3
1 Allgemeine Vorschriften.....	3
1.1 Gültigkeit	3
1.2 Alleinige Vereinbarung und Schriftform	3
2 Auftragsverarbeitung nach Art. 28 DSGVO.....	4
2.1 Grundsätze der Datenverarbeitung.....	4
2.2 Rechte und Pflichten des Auftraggebers.....	5
2.3 Rechte und Pflichten des Auftragnehmers.....	6
2.4 Datenschutzorganisation.....	8
2.5 Technische und organisatorische Maßnahmen	8
2.6 Prüfungsrecht	9
2.7 Unterauftragnehmer	9
2.8 Haftung	10
3 Schlussbestimmungen.....	10
Anlage 1: Technische und organisatorische Maßnahmen	11
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO).....	11
2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)	12
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO).....	13
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)	13

Präambel

Der Auftraggeber erteilt dem Auftragnehmer mit dem Hauptvertrag einen Auftrag zur Datenverarbeitung. Um den Hauptvertrag datenschutzrechtlich zu begleiten ist es erforderlich, eine Vereinbarung zur Auftragsverarbeitung zu schließen. Vor diesem Hintergrund schließen die Parteien folgende Vereinbarung:

1 Allgemeine Vorschriften

1.1 Gültigkeit

- a. Diese Datenschutzvereinbarung (nachfolgend: DSV) tritt mit ihrer Unterzeichnung in Kraft. Sie ist eine eigenständige Vereinbarung zwischen den Parteien und steht neben dem zwischen den Parteien geschlossenen Hauptvertrag. Wenn und soweit der Hauptvertrag Regelungen enthält, die denjenigen der DSV entgegenstehen, so haben die Regelungen der DSV Vorrang, soweit in der DSV nicht etwas anderes geregelt ist.

1.2 Alleinige Vereinbarung und Schriftform

- a. Diese DSV ersetzt alle bisherigen Vereinbarungen zur Auftragsdatenverarbeitung zwischen den Parteien. Die Regelungen der DSV sind abschließend.
- b. Jede Änderung bedarf der Schriftform. Das Schriftformerfordernis gilt nicht für die Aktualisierung der Anlagen, hier ist die Textform (auch per E-Mail) ausreichend. Jede Änderung der Anlagen benötigt für ihre Wirksamkeit die Bestätigung durch die jeweils andere Partei in Textform (auch per E-Mail).

2 Auftragsverarbeitung nach Art. 28 DSGVO

2.1 Grundsätze der Datenverarbeitung

- a. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des für die Datenverarbeitung verantwortlichen Auftraggebers (Auftragsverarbeitung). Personenbezogene Daten werden vom Auftragnehmer nur in dem im Hauptvertrag beschriebenen Umfang und ausschließlich zu dem dort geregelten Zweck verwendet. Umfang, Art und Zweck der vorgesehenen Verarbeitung sind wie folgt festgelegt:

Gegenstand und Dauer der Datenverarbeitung sind wie folgt geplant:

Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Auftrag, Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

Die Dauer der Verarbeitung entspricht der im Auftrag vereinbarten Laufzeit.

Ergänzend wird auf die Leistungsbeschreibung des Hauptvertrags verwiesen.

Art und Zweck der Datenverarbeitung sind wie folgt geplant:

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.

Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung im Bereich Cloud Dienstleistungen, Hosting, Software as a Service (SaaS) und IT-Support erforderlichen Zwecke.

Die Datenverarbeitung umfasst die folgenden Arten personenbezogener Daten:

Generell werden alle Datenarten durch die Veröffentlichung im eigenen Content verarbeitet.

Im Besonderen:

- Stammdaten (bspw. benötigt für Login, Identifizierung o.ä.)
- Vertragsdaten (Selbstverwaltung des Hauptvertrages und Auftragsverarbeitungsvereinbarung)
- Kontaktdaten (nur bei Eingabe im Content Ihrer eigenen Veröffentlichung)
- Kommunikationsdaten (nur bei Eingabe im Content Ihrer eigenen Veröffentlichung)
- Personaldaten (nur bei Eingabe im Content Ihrer eigenen Veröffentlichung)
- Kundendaten (nur bei Eingabe im Content Ihrer eigenen Veröffentlichung)

Die Verarbeitung umfasst die folgenden Kategorien betroffener Personen:

Im Detail:

- Mitarbeiter/Dienstleister
- Kunden
- Lieferanten
- Interessenten
- Bewerber

- b.** Die Verarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in Staaten, auch durch einen Unterauftragnehmer des Auftragnehmers, außerhalb der EU / des EWR bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen von Kapitel 5 DSGVO erfüllt sind. Die Beauftragung von Unterauftragnehmern richtet sich nach Ziffer 2.7.
- c.** Es gelten die Definitionen der DSGVO.

2.2 Rechte und Pflichten des Auftraggebers

- a.** Der Auftraggeber ist für den Schutz der Rechte und Freiheiten der betroffenen Personen verantwortlich. Er erteilt dem Auftragnehmer die für den Schutz der Rechte und Freiheiten erforderlichen Weisungen. Er stellt sicher, dass von ihm an den Auftragnehmer erteilte Weisungen alle notwendigen Informationen enthalten, die der Auftragnehmer für die datenschutzkonforme Durchführung der Auftragsverarbeitung benötigt.
- b.** Der Auftraggeber ist für die Vereinbarkeit der von ihm an den Auftragnehmer erteilten Weisungen mit den jeweils für die Verarbeitung einschlägigen rechtlichen Anforderungen verantwortlich. Die Pflichten des Auftragnehmers zur selbstständigen Gestaltung von Verarbeitungsvorgängen nach Ziffer 2.3.m. bleiben unberührt.
- c.** Der Auftraggeber weist den Auftragnehmer hiermit an, selbstständig keine Zweckänderung der Datenverarbeitung durchzuführen und die personenbezogenen Daten, die ihm vom Auftraggeber zum Zwecke der Datenverarbeitung zur Verfügung gestellt werden oder die ihm während der Durchführung, als Ergebnis der Datenverarbeitung oder auf sonstige Weise bekannt werden, nicht für eigene Zwecke zu verwenden. Dies gilt auch für die Verwendung pseudonymisierter oder anonymisierter Daten, es sei denn der Auftraggeber hat der Verwendung der Daten zugestimmt. Im Falle der Zustimmung hat der Auftraggeber sicherzustellen, dass die gesetzlichen Anforderungen an eine derartige Nutzung der Daten erfüllt sind.
- d.** Soweit dies für die Nutzung der Datenverarbeitung erforderlich ist, holt der Auftraggeber eine den gesetzlichen Anforderungen genügende Einwilligung der betroffenen Personen ein. Der Auftragnehmer ist nicht berechtigt, selbstständig Einwilligungen von betroffenen Personen einzuholen und diese Einwilligung zur Voraussetzung für die Nutzung seiner Dienste durch die betroffenen Personen zu machen.
- e.** Der Auftraggeber ist berechtigt, dem Auftragnehmer die Ausgestaltung der Datenverarbeitung zur Erfüllung des Auftrags zu überlassen, solange der Auftragnehmer die in Ziffer 2.3.m. genannten Anforderungen beachtet.

- f.** Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei den Verarbeitungsergebnissen feststellt, insbesondere wenn er Grund zu der Annahme hat, dass die Art und Weise der Verarbeitung der Daten durch den Auftragnehmer gegen datenschutzrechtliche Anforderungen verstößt.
- g.** Der Auftraggeber erfüllt alle Pflichten zur Wahrung der Informations-, Auskunfts- und sonstigen Rechte der betroffenen Personen, die sich aus den jeweils für die Verarbeitung gültigen Rechtsgrundlagen ergeben.
- h.** Der Auftraggeber erstellt und pflegt die Dokumentation der Datenverarbeitung in seiner Verfahrensübersicht und führt, soweit erforderlich, die Datenschutzfolgenabschätzung für die Verarbeitung durch.

2.3 Rechte und Pflichten des Auftragnehmers

- a.** Der Auftragnehmer ist verpflichtet, personenbezogene Daten, die ihm im Rahmen des Auftrags vom Auftraggeber zum Zwecke der Datenverarbeitung zur Verfügung gestellt werden oder die ihm während der Durchführung, als Ergebnis der Datenverarbeitung oder auf sonstige Weise bekannt werden, nur entsprechend den Weisungen des Auftraggebers zu verarbeiten. Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich darauf hinzuweisen, wenn er der Ansicht ist, dass eine vom Auftraggeber erteilte Weisung gegen geltendes Datenschutzrecht verstößt. Die Verarbeitung kann in diesem Fall verweigert werden.

- b.** Der Auftragnehmer erklärt, dass er aufgrund gesetzlicher Anforderungen der Europäischen Union oder eines Mitgliedsstaats der Europäischen Union nicht verpflichtet ist, Daten auch ohne Weisung des Auftraggebers zu verarbeiten.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er dennoch eine entsprechende Aufforderung zur Datenverarbeitung erhält. Dies gilt nicht, wenn der Auftragnehmer aufgrund gesetzlicher Vorschriften zur Geheimhaltung verpflichtet ist.

- c.** Der Auftragnehmer darf Daten nach Ziffer 2.3.a. nicht an Dritte mit Sitz außerhalb der EU / des europäischen Wirtschaftsraums offenlegen, es sei denn, der Auftraggeber hat explizit der Offenlegung schriftlich zugestimmt. Dies gilt nicht, soweit die Veranlassung der Offenlegung in der Verantwortung des Auftraggebers liegt und der Auftragnehmer hierauf keinen Einfluss hat.
- d.** Der Auftragnehmer versichert, dass ihm alle einschlägigen datenschutzrechtlichen Vorschriften, die zu einer rechtmäßigen Durchführung der Datenverarbeitung erforderlich sind, bekannt sind und gewährleistet deren Umsetzung, soweit er hierzu nach dieser Vereinbarung oder einer gesetzlichen Anforderung verpflichtet ist. Er gewährleistet, dass alle von ihm mit der Durchführung des Auftrags beauftragten Personen vor dem Beginn der Verarbeitung zur Vertraulichkeit verpflichtet worden sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtungen gelten über das Vertragsende hinaus.

Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten.

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

- e.** Soweit der Auftragnehmer aus technischen oder tatsächlichen Gründen nicht in der Lage ist, von der Verarbeitung betroffene personenbezogene Daten zu berichtigen, zu sperren oder zu löschen, ist der Auftraggeber dazu verpflichtet, den Auftragnehmer bei der Durchführung der jeweiligen Maßnahme zu unterstützen. Der Auftragnehmer berichtigt, löscht oder sperrt Daten nach Ziffer 2.3.a. grundsätzlich nur auf Weisung des Auftraggebers. Die Beendigung des Auftragsverhältnisses nach Ziffer 2.3.f. bleibt unberührt.

- f.** Nach Beendigung des Auftragsverhältnisses hat der Auftragnehmer etwaige noch nicht übergebene personenbezogene Daten nach Ziffer 2.3.a. nach Maßgabe des Auftraggebers an ihn zu übergeben oder zu löschen. Spätestens mit Beendigung des Hauptvertrags sowie nach Ablauf der dort gegebenenfalls vereinbarten Aufbewahrungsfristen sind alle personenbezogenen Daten aus dem Auftragsverhältnis zu löschen, es sei denn, dass der Auftragnehmer nachweisen kann, dass er aufgrund gesetzlicher Vorschriften zur Aufbewahrung der personenbezogenen Daten verpflichtet ist.
- g.** Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen, damit die Daten des Auftraggebers rechtzeitig von den DV-Systemen des Auftragnehmers genommen werden können.
- h.** Wenn und soweit der Auftraggeber im Zusammenhang mit der Verarbeitung von Daten nach Ziffer 2.3.a. eine Anfrage einer Aufsichtsbehörde oder sonstigen zuständigen Stelle erhält, hat er den Auftragnehmer unverzüglich zu informieren und die Anfrage unverzüglich weiterzuleiten.
- i.** Der Auftragnehmer gewährleistet seinerseits die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Der Auftraggeber wird dem Auftragnehmer den insoweit entstehenden Aufwand vergüten, sofern dies nach geltendem Datenschutzrecht zulässig ist.
- j.** Sollten betroffene Personen oder sonstige Dritte datenschutzrechtliche Anfragen an den Auftragnehmer richten oder Datenschutzrechte gegenüber dem Auftragnehmer geltend machen, die Daten nach Ziffer 2.3.a. betreffen, leitet der Auftragnehmer diese Anfragen unverzüglich an den Auftraggeber weiter. Der Auftraggeber wird dem Auftragnehmer den insoweit entstehenden Aufwand vergüten, sofern dies nach geltendem Datenschutzrecht zulässig ist.
- k.** Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Verletzungen des Datenschutzes bzw. der im Vertrag getroffenen Festlegungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.
- l.** Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten unrechtmäßig offengelegt wurden, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/ der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Offenlegung künftig zu verhindern. Der Auftragnehmer wird an der Aufklärung des Vorfalls und der Umsetzung von Gegenmaßnahmen in vollem Umfang mitwirken.

- m.** Wenn und soweit der Auftragnehmer plant, im Rahmen oder neben der beauftragten Datenverarbeitung weitere Daten zur eigenen Verwendung zu erheben oder sonst zu verarbeiten (z.B. Nutzungsdaten seiner Dienste, die von Mitarbeitern des Auftraggebers genutzt werden), bedarf dies der Zustimmung des Auftraggebers. Beruht diese Datenerhebung auf einer gesetzlichen Erlaubnis, z.B. die Bildung pseudonymer Nutzungsprofile auf Basis eines Widerspruchsrechts der betroffenen Person, so hat der Auftragnehmer den Auftraggeber vor der technischen Umsetzung der Verarbeitung über diese Maßnahmen zu informieren. Der Auftragnehmer ist verpflichtet, alle gesetzlichen Anforderungen an eine derartige Verarbeitung und insbesondere die gesetzlichen Widerspruchs-, Auskunfts- und Informationsrechte der betroffenen Personen zu beachten und diesen gegenüber wahrzunehmen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Nachfrage die Einhaltung der gesetzlichen Anforderungen an die Verarbeitung nachzuweisen. Der Auftraggeber ist berechtigt, die Durchführung einer derartigen Verarbeitung zu untersagen, wenn der Auftragnehmer diesen Nachweis nicht erbringen kann. Der Auftragnehmer darf die Nutzung seiner Dienste durch Mitarbeiter, Geschäftspartner, Kunden oder sonstige betroffene Personen, die nach dem Hauptvertrag zur Nutzung der Dienste des Auftragnehmers berechtigt sind, von der Einwilligung in eine derartige Datenverarbeitung abhängig machen.
- n.** Wenn und soweit dem Auftragnehmer die Ausgestaltung der Datenverarbeitung nach Ziffer 2.2.e. überlassen ist, verpflichtet sich der Auftragnehmer, die jeweilige Ausgestaltung nach den Vorgaben der DSGVO durchzuführen. Insbesondere hat der Auftragnehmer die Vorgaben von Art. 25 DSGVO zu beachten und dem Auftraggeber auf Verlangen die Einhaltung dieser Vorgaben auf geeignete Art und Weise nachzuweisen. Der Nachweis kann durch ein genehmigtes Zertifizierungsverfahren gem. Art. 42 DSGVO erbracht werden.

2.4 Datenschutzorganisation

- a.** Der Auftragnehmer bestellt, soweit er hierzu verpflichtet ist, einen Datenschutzbeauftragten. Ist der Auftragnehmer zur Bestellung eines Datenschutzbeauftragten nicht verpflichtet, so benennt er den in seiner Organisation für den Datenschutz zuständigen Verantwortlichen.
- b.** Der Auftraggeber hat das Recht, den Datenschutzbeauftragten oder Datenschutzverantwortlichen jederzeit in Datenschutzangelegenheiten, die die DSV betreffen, zu kontaktieren unter privacy@bendelschrade.de

2.5 Technische und organisatorische Maßnahmen

- a.** Der Auftragnehmer bietet hinreichende Garantien, dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit der DSGVO und den Rechten der betroffenen Person steht
- b.** Der Auftragnehmer gewährleistet selbstständig die Umsetzung der technischen und organisatorischen Maßnahmen nach Ziffer 2.5.a. Der Stand zum Zeitpunkt des Abschlusses der DSV wird am Ende dieser Vereinbarung als Anlage 1 dokumentiert.
- c.** Der Auftragnehmer darf keine Veränderung vornehmen, die die in Anlage 1 dokumentierten Anforderungen wesentlich unterschreitet. Der Auftragnehmer hat den Auftraggeber über maßgebliche Veränderungen der technischen und organisatorischen Maßnahmen zu informieren.
- d.** Sollte eine Änderungsanforderung des Auftraggebers auf einer Weisung oder Empfehlung einer für die Datenverarbeitung zuständigen Aufsichtsbehörde beruhen oder ein Vorfall nach Ziffer 2.3.I. vorausgegangen sein, ist eine Anpassung der technischen und organisatorischen Maßnahmen durch den Auftragnehmer erforderlich.

2.6 Prüfungsrecht

- a. Der Auftragnehmer berechtigt den Auftraggeber, zu den üblichen Geschäftszeiten die Einhaltung der Vorschriften über den Datenschutz und der von ihm getroffenen Weisungen zu überprüfen. Der Auftraggeber wird den Auftragnehmer vorab mindestens 4 Wochen vor Durchführung über die geplante Überprüfung informieren.
- b. Der Auftragnehmer räumt dem Auftraggeber hierzu ein umfassendes Auskunfts- und Einsichtsrecht, sowie in Abstimmung mit dem Auftragnehmer ein Zutritts- und Zugangsrecht zu den relevanten Geschäftsräumen des Auftragnehmers einschließlich der Räumlichkeiten der Datenverarbeitung ein, wobei der Auftraggeber bei Ausübung dieser Rechte auf die betrieblichen Belange des Auftragnehmers Rücksicht nehmen muss. Bei diesen Kontrollen wirkt der Auftragnehmer im hierzu erforderlichen Umfang mit. Diese Pflicht besteht bereits vor dem Beginn der Datenverarbeitung und kann vom Auftraggeber wiederholt eingefordert werden, allerdings nur sofern begründeter Anlass für eine erneute Überprüfung vorliegt.
- c. Die Durchführung der Prüfung kann nach Ermessen des Auftraggebers durch den Nachweis der Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO ersetzt werden.
- d. Der Auftraggeber ist berechtigt, für die Durchführung der Prüfung sachkundige externe Dritte einzusetzen, die von Berufs wegen oder aufgrund einer vertraglichen Vereinbarung zur Verschwiegenheit verpflichtet sind. Die Kosten solcher zusätzlichen Überprüfungen sind vom Auftraggeber zu tragen.
- e. Der Auftraggeber wird dem Auftragnehmer die durch die Prüfungen gemäß Ziffer 2.6. entstehenden Aufwände vergüten, sofern dies nach geltendem Datenschutzrecht zulässig ist.

2.7 Unterauftragnehmer

- a. Die Beauftragung von Unterauftragnehmern ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftragnehmer teilt dem Verantwortlichen jeden neuen Unterauftragsverarbeiter mit, bevor er diesen beauftragt, personenbezogene Daten im Zusammenhang mit der Erbringung der betreffenden Dienstleistungen zu verarbeiten. Der Verantwortliche kann innerhalb von 2 Wochen nach der Information seine Zustimmung erteilen oder der Verwendung des neuen Unterauftragsverarbeiters widersprechen. Nach Ablauf dieser Frist gilt der neue Unterauftragnehmer als genehmigt. Im Falle des Widerspruchs kann der Auftragnehmer die anwendbaren Dienstleistungsverträge kündigen, wenn und soweit er die Dienstleistungen nicht ohne den Einsatz des neuen Unterauftragsverarbeiters erbringen kann. Der Auftragnehmer setzt zum Zeitpunkt des Abschlusses dieser Vereinbarung die im folgenden genannten Unterauftragnehmer ein:

Vollständige Firmierung des Unterauftragnehmers	Anschrift	Land	Beschreibung der Leistung
STRATO AG	Pascalstraße 10, 10587 Berlin	Deutschland	Cloud-Dienstleistungen, Hosting, SaaS, IT Support

- b. In der schriftlichen Vereinbarung mit dem Unterauftragnehmer stellt der Auftragnehmer sicher, dass die in diesem Auftragsverarbeitungsvertrag vereinbarten Regelungen auch im Verhältnis zwischen Auftragnehmer und Unterauftragnehmer gelten.
- c. Der Auftragnehmer haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

2.8 Haftung

Auftraggeber und Auftragnehmer haften im Rahmen ihrer Verantwortlichkeiten gemäß den gesetzlichen Bestimmungen des Art. 82 DSGVO gegenüber Dritten für Schäden, die durch eine nicht der DSGVO entsprechenden Datenverarbeitung entstanden sind.

3 Schlussbestimmungen

Wenn und soweit Vorgaben der Aufsichtsbehörden und/oder zusätzliche gesetzliche Vorgaben die Änderung von Bestimmungen der DSV und/oder der zugehörigen Anlagen erforderlich machen, sind die Parteien verpflichtet, an der Umsetzung der Anforderungen und der Aufnahme in die DSV mitzuwirken. Vorgaben der für die vom Auftrag umfasste Datenverarbeitung zuständigen Aufsichtsbehörde oder einer sonstigen zuständigen offiziellen Stelle sind dabei als verbindlich zu betrachten.

AUFTRAGNEHMER

Name _____

Funktion _____

Ort, Datum und Unterschrift

Übersicht Anlagen

Anlage	Inhalt
Anlage 1	Technische und organisatorische Maßnahmen

Anlage 1: Technische und organisatorische Maßnahmen

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

■ Zutrittskontrolle

- Zutrittskontrolle zu Gebäuden und Räumen
- Zutritt und Aufenthalt von Besuchern nur unter Begleitung
- Vergabe, Kontrolle und Entzug von Zutrittsrechten nach Need-To-Know Prinzip
- Zutrittskonzept für gesonderte Räume wie z.B. Serverräume
- Verpflichtung von Dienstleistern mit Zutritt auf Einhaltung des Datenschutzes
- Zutrittsliste für Besucher
- Zutritt des Reinigungspersonal und Wartungspersonal
- Zutrittsberechtigungen definiert und dokumentiert, z.B. Protokollierung
- Stark eingeschränkte Zutrittsberechtigungen
- Alarmanlage, Wachdienst, Videoüberwachung
- Dokumentation / Protokollierung von Schließanlage (Wer hat eine Chipkarte?/ Wer hat wann zugegriffen?)
- Regelungen zu Entsorgung von Dokumenten, Shredder, Datenschutzcontainer
- Durch ISO 27001 Zertifizierung:
 - Besucherregelung
 - Physische Absicherung von Gebäuden und Räumen, z.B. Umzäunung, Türen

■ Zugangskontrolle

- Zugang über persönliche Benutzerkonten mit Passwort-Schutz
- Systemseitige Sperrung bei fehlerhaften Anmeldeversuchen
- Vergabe, Kontrolle und Entzug von Berechtigungen
- Berechtigungskonzepte für IT-Systeme, Anwendungen und Daten
- Automatische Bildschirmsperre
- Löschung und Entsorgung von Daten und IT-Equipment
- Firewall-Konzept
- Durch ISO 27001 Zertifizierung:
 - Prozess zur Vergabe, Änderung und Deaktivierung von Benutzerkonten nachdem Mehraugen-Prinzip
 - Regelmäßige Passwortänderung
 - Passwortkomplexität,-länge und-wechsel
 - Awareness / Schulungen
 - Externer Zugriff auf das Unternehmensnetzwerk
 - Malware Schutz
 - Regelmäßige Überprüfung von Benutzerkonten
 - Rollenbasierte Administration
 - Härtung von Systemen
 - Interne Audits
 - Change Management

- Wartung von IT-Systemen
- Patch Management
- Überwachung und Protokollierung von Berechtigungsänderungen
- Passwortsicherheit für Systemkonten

■ Zugriffskontrolle

- Rechte und Rollenkonzepte
- Need-to-Know Prinzip
- Prozess zur Vergabe, Änderung und Deaktivierung von Zugriffsrechten nach dem Need-To-Know Prinzip
- Zugriffskonzepte für IT-Systeme, Anwendungen und Daten
- Löschkonzept
- Netzwerksicherheitsfunktionen z.B. Port Security
- Netzwerksegmentierung
- Verschlüsselte Kommunikationswege
- Zonen-und Stufenkonzept z.B. DMZ, Reverse Proxy
- Überwachung von Zugriffen
- Verschlüsselung von IT-Systemen, Anwendungen, Datenbanken, Übertragungswege
- Durch ISO 27001 Zertifizierung:
 - Rechtekonzept für IT-Administratoren
 - Protokollierung von Zugriffen und administrativen Tätigkeiten
 - Zugriffsschutz für Datensicherungen
 - Protokollierung von Zugriffen
 - Regelmäßige Überprüfung von Zugriffsberechtigungen
 - Schwachstellenprüfung (externe Verbindungen)
 - Durchführung von Sicherheitsüberprüfungen
 - Multifaktorauthentifizierung bei externem Zugriff
 - IDS / IPS
 - Schwachstellenmanagement

■ Trennungskontrolle

- Logische Trennung von Daten z.B. Mandantenfähigkeit in Anwendungen
- Trennung von Produktiv-und Test-Systemen
- Berechtigungen zur Steuerung des Zugriffs auf Daten

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

■ Weitergabekontrolle

- Verschlüsselung des Mailverkehrs (extern) und Verschlüsselung von Speichermedien
- Organisatorische Regelungen zur Verhinderung der Weitergabe
- Schulungen im Kontext Datenschutz
- Verschlüsselte Speichermedien
- Protokollierung der Weitergabe
- Schutz der Datensicherungen z.B. durch Verschlüsselung
- Verschlüsselung von Übertragungswegen

- Durch ISO 27001 Zertifizierung:
 - Sicherer physischer Transport
 - Protokollierung von Fernzugriffen

■ Eingabekontrolle

- Protokollierung von Eingaben, Änderungen und Löschungen
- Systemseitige Einschränkung der Schreib- und Löschrechte

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

■ Verfügbarkeitskontrolle

- Schulung von Mitarbeitern des Auftragnehmers
- Vereinbarungen zur Auftragsdatenverarbeitung mit Subunternehmern
- Verpflichtung von Subauftragnehmern auf Datenschutzkonzept
- Prüfpflicht des Auftragnehmers von Subauftragnehmern
- Durch ISO 27001 Zertifizierung:
 - SLAs mit Dienstleistern
 - Monitoring von IT-Systemen
 - Netzwerkplan, IT-Asset Management
 - Verfügbarkeit von Fachpersonal
 - Auslagerung der Datensicherung
 - Überwachung von Umgebungsparametern z.B. Temperatur, Luftfeuchtigkeit
 - Vertretungsregelungen
 - Klimatisierung
 - Wartung der Versorgungseinrichtungen
 - Überwachung der technischen Versorgungsinfrastruktur (Klima, USV, NSV)

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

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

■ Datenschutz-Management;

■ Incident-Response-Management;

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

■ Auftragskontrolle

- Schulung von Mitarbeitern des Auftragnehmers
- Vereinbarungen zur Auftragsdatenverarbeitung mit Subunternehmern
- Verpflichtung von Subauftragnehmern auf Datenschutzkonzept
- Prüfpflicht des Auftragnehmers von Subauftragnehmern