**Auftragsverarbeitungsvertrag**

gemäß

**Artikel 28 DSGVO**

zwischen

**visuSolution GmbH**

**Lüderitzer Weg 6**

**39517 Tangerhütte OT Brunkau**

- nachfolgend als Auftragnehmer bezeichnet -

und

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

- nachfolgend als Auftraggeber bezeichnet -

**Präambel**

Dieser Vertrag

* basiert auf dem zwischen den Parteien bestehenden Hauptvertrag vom \_\_\_\_\_\_\_\_\_\_\_\_;
* findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Subunternehmer/Unterauftragnehmer gemäß Anlage 1 dieses Vertrages personenbezogene Daten des Auftraggebers verarbeiten;
* regelt die Rechte und Pflichten von Auftraggeber und -nehmer, nachfolgend als *Parteien* bezeichnet, im Rahmen der Verarbeitung von personenbezogenen Daten im Auftrag.
* ersetzt falls vorhanden alle vorherigen Auftragsverarbeitungsverträge zwischen den Parteien. Die vorherigen Verträge verlieren mit der Unterzeichnung dieses Vertrages ihre Gültigkeit.

In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung, nachfolgend als DSGVO bezeichnet, zu verstehen.

In diesem Sinn ist der Auftraggeber der Verantwortliche, der Auftragnehmer der Auftragsverarbeiter.

Soweit Erklärungen nachfolgend schriftlich zu erfolgen haben, handelt es sich um die Schriftform gemäß § 126 BGB.

Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

Dieser Vertrag regelt ausschließlich die ausdrücklich aufgeführten Punkte.

Für alle in diesem Vertrag nicht geregelten Punkte gelten die Bestimmungen des Hauptvertrages.

Erst soweit im Hauptvertrag auch keine Regelung getroffen ist, gilt das Gesetz.

**§ 1 Dauer der Verarbeitung**

Dieser Auftragsverarbeitungsvertrag beginnt unmittelbar mit Unterzeichnung und gilt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrages durch eine der beiden Parteien.

**§ 2 Gegenstand der Verarbeitung**

Durchführung von Fernwartungen, Support und Service auf den IT-Systemen des Auftraggebers und für die Produkte, die der Auftraggeber beim Auftragnehmer erworben hat.

**§ 3 Art und Zweck der Verarbeitung**

1. Die Verarbeitungen finden zu folgenden Zwecken statt:

* Aktualisieren der Gerätetreiber per Fernwartung mittels TeamViewer-Software
* Ausführen von Installation / Neuinstallationen
* Fehleranalysen der visuReal®-Software durch schrittweises nachvollziehen der Mess- und Eingabehistorie anhand von Kundendaten
* Prüfen der Einstellung von visuReal®
* Prüfen der Kamerasäule samt Treiber / AMCAP/ Stream Catcher

1. Betroffene Personen der Verarbeitung sind:

* Kunden des Auftraggebers

1. Verarbeitet werden unter anderem folgende Daten der Kunden:
2. Normale Daten gemäß Art. 6 DSGVO:

* Fassung
* Glashersteller
* IP-Adresse
* Kommunikationsdaten
* Kundenhistorie
* Personenstammdaten
* Vertragsstammdaten
* Zugriffsrechte

1. Besonders schützenswerte Daten gemäß Art. 9 DSGVO:

* Dioptrien
* Glasarten
* Hornhaut-Scheitel-Abstand
* Kopfdrehung
* Kopfneigung
* Pupillendistanz
* Rezeptglasdaten

**§ 4 Allgemeine Pflichten des Auftragnehmers und Weisungsgebundenheit**

1. Der Auftraggeber hat hinsichtlich der Verarbeitung im Auftrag gegenüber dem Auftragnehmer ein Weisungsrecht.
2. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen, sperren oder weiterleiten.
3. Den entsprechenden schriftlichen Weisungen des Auftraggebers gemäß § 9 Abs. 3 und Anlage 3 dieses Vertrages wird der Auftragnehmer jederzeit Folge leisten.
4. Der Auftragnehmer
5. wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Bestimmungen verstößt.
6. ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.
7. hat ihm erteilte Weisungen und deren Umsetzung schriftlich zu dokumentieren.
8. verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet.

Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten.

1. verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen - insbesondere nicht für eigene - Zwecke.
2. bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind.

Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung und wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten.

Eine physische Trennung ist nicht zwingend erforderlich.

1. verpflichtet sich, die Vertraulichkeit bei der Verarbeitung streng zu wahren.

Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

In diesem Zusammenhang sichert der Auftragnehmer zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden.

Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen.

1. trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
2. leitet alle an ihn gerichteten Anfragen unverzüglich an den Auftraggeber weiter.
3. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
4. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen, oder machen betroffene Personen gegen ihn Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
5. Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen.
6. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz.

In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden.

Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde.

Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

1. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR.

Jegliche Verlagerung in ein Drittland darf nur mit ausdrücklicher Zustimmung des Auftraggebers und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie unter Einhaltung der Bestimmungen dieses Vertrags erfolgen.

**§ 5 Mitteilungspflichten des Auftragnehmers**

1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit.

Auch begründete Verdachtsfälle sind mitzuteilen.

1. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen.
2. Sie muss mindestens folgende Angaben enthalten:
3. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
4. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien, der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
5. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;
6. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.
7. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragsdurchführung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
8. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese einen Bezug zur Auftragsverarbeitung aufweisen.
9. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

**§ 6 Subunternehmer und Unterauftragsverhältnisse**

1. Der Auftragnehmer ist berechtigt, zum Zweck der Erfüllung dieses Vertrages, Subunternehmer bzw. Unterauftragsverarbeiter zu beauftragen.
2. Die Beauftragung von Subunternehmern ist nur zulässig, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die mit den in diesem Vertrag vereinbarten Pflichten vergleichbar sind.
3. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
4. Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können.

Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchführen zu können oder durch Dritte durchführen zu lassen.

1. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
2. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
3. Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer schriftlich dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat.
4. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich auf dem Gebiet der EU oder des EWR erbringen, ist nicht zulässig.
5. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen.
6. Die Prüfung und ihr Ergebnis sind so aussagekräftig schriftlich zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind.
7. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.
8. Unterauftragsverhältnisse im Sinne dieses Vertrages sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen.

Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservices sind nicht erfasst.

1. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt hiervon unberührt.
2. Zurzeit sind die in der Anlage 1 zu diesem Vertrag mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt.
3. Der Auftragnehmer wird den Auftraggeber während der Vertragslaufzeit über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern bzw. Unterauftragsverarbeitern informieren.

Diese Information wird dem Auftraggeber gemäß Art. 28 Abs. 9 DSGVO schriftlich zur Verfügung gestellt; die Information kann auch in einem elektronischen Format übermittelt werden.

1. Der Auftraggeber hat gemäß Art. 28 Abs. 2 Satz 2 nach Erhalt der vorstehenden Information die Möglichkeit, gegen die beabsichtigte Änderung mit einer Frist von 4 Wochen ab Erhalt der Information Einspruch zu erheben.

Nach dem Einspruch des Auftraggebers haben beide Vertragsparteien das Recht, das Vertragsverhältnis ab Zugang des Einspruchs mit einer Frist von 4 Wochen zu kündigen.

1. Erfolgt innerhalb der in Satz 1 genannten Frist von 4 Wochen kein Einspruch des Auftraggebers, gilt die Zustimmung des Auftraggebers zur Beauftragung des weiteren Subunternehmers bzw. Unterauftragsverarbeiters als erteilt.

**§ 7 Technische und organisatorische Maßnahmen**

1. Die in der Anlage 2 zu diesem Auftragsverarbeitungsvertrag beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt.
2. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
3. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, soweit Änderungen an technische und rechtliche Gegebenheiten erforderlich werden.

Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen.

1. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen.
2. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen.
3. Soweit die getroffenen Sicherheitsmaßnahmen den ursprünglichen Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Eine physische Trennung ist jedoch nicht zwingend erforderlich.

1. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

1. Die Verarbeitung von Daten in Privatwohnungen (Homeoffice) ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet.

Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit gewährleistet ist und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können.

1. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.
2. Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung.

Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein.

Sämtliche Ein- und Ausgänge werden schriftlich dokumentiert.

1. Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit.

Der Nachweis kann auch durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

**§ 8 Pflichten bei Beendigung des Vertrages**

1. Bei Beendigung des Auftragsverhältnisses, oder jederzeit auf Verlangen des Auftraggebers, hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben.

Ebenfalls zu vernichten sind sämtliche vorhandenen Kopien der Daten.

1. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

Eine physische Vernichtung erfolgt gemäß DIN 66399.

1. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
2. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
3. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren.

Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

**§ 9 Rechte und Pflichten des Auftraggebers**

1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen schriftlich und dokumentiert diese.
3. Der Auftraggeber ist verpflichtet, die weisungsberechtigten Personen mit der Anlage 3 zu diesem Vertrag namentlich und konkret zu benennen.
4. In dringenden Fällen können Weisungen durch die vom Auftraggeber konkret benannten Personen gegenüber dem Auftragnehmer auch mündlich erteilt werden.

Solche Weisungen wird der Auftraggeber unverzüglich schriftlich bestätigen und dokumentieren.

1. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
2. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst, oder durch geeignete Dritte, insbesondere durch die Einholung von Auskünften, die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme, sowie sonstige Kontrollen unter folgenden Maßgaben vor Ort zu kontrollieren:
3. Den mit der Kontrolle betrauten Personen oder geeigneten Dritten, die der Auftraggeber gemäß Anlage 3 dieses Vertrages namentlich und konkret benannt hat, ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen.
4. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
5. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen.
6. Soweit nicht aus vom Auftraggeber schriftlich zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.
7. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

**§ 10 Sonderkündigungsrecht**

1. Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist außerordentlich kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführt oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in diesem Vertrag bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

**§ 11 Sonstige Bestimmungen**

1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch nach Beendigung des Vertrages dauerhaft und unbefristet vertraulich zu behandeln.
2. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei vertraulich zu behandeln.
3. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, beispielsweise durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

**§ 12 Schlussbestimmungen**

1. Dieser Vertrag ersetzt frühere Fassungen mit Wirkung ab dem Tag des Abschlusses.
2. Erfüllungsort für alle Leistungen des Auftragnehmers ist der Sitz des Auftragnehmers.
3. Änderungen oder Ergänzungen zu diesem Vertrag bedürfen der Schriftform. Dies gilt auch für die Abbedingung des Schriftformerfordernisses.
4. Sollten Bestimmungen dieses Vertrages unwirksam oder nichtig sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.
5. Die Parteien verpflichten sich, die unwirksame oder nichtige Bestimmung durch eine solche zu ersetzen, die dem mit der unwirksamen oder nichtigen Bestimmung wirtschaftlich Gewollten am nächsten kommt.
6. Gerichtsstand für Streitigkeiten aus diesem Vertrag ist der Sitz der Auftragnehmers.

**§ 13 Bestätigungen**

Die Vertragsparteien bestätigen mit Ihrer Unterschrift, über den Inhalt des heutigen Vertrages einig zu sein und jeweils eine unterschriebene Ausfertigung des Vertrages nebst der Anlage 1 *Subunternehmer/Unterauftragnehmer*, der Anlage 2 *Technische und organisatorische Maßnahmen* sowie der Anlage 3 *Personen mit Weisungsbefugnis + Personen/Dritte mit Kontrollrechten* erhalten zu haben.

Tangerhütte, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Ort, Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Unterschrift und Stempel Auftragnehmer Unterschrift und Stempel Auftraggeber

**Anlage 1**

zum

**Auftragsverarbeitungsvertrag**

zwischen

**visuSolution GmbH**

**Lüderitzer Weg 6**

**39517 Tangerhütte OT Brunkau**

- nachfolgend als Auftragnehmer bezeichnet -

und

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

- nachfolgend als Auftraggeber bezeichnet -

**Subunternehmer / Unterauftragnehmer**

|  |  |  |
| --- | --- | --- |
| **Firma** | **Anschrift / Land** | **Beschreibung der Leistung** |
| 123Altmark Agentur GbR | Breite Straße 68  39576 Stendal  Deutschland | Erstellung und Pflege  Unternehmens-Webseite |
| hansa Büroorganisation & Datensysteme GmbH | Beelitzer Weg 2  39596 Arneburg  Deutschland | Wartung und Pflege  Angebotssoftware |
| Sendinblue GmbH | Köpenicker Straße 126  10179 Berlin  Deutschland | Newsletterversand |
| Ollendorf Mess-Systeme | Zur Springe 5  39517 Tangerhütte  Deutschland | Entwicklung und technische Betreuung Hard-/Software optische Geräte |

**Anlage 2**

zum

**Auftragsverarbeitungsvertrag**

zwischen

**visuSolution GmbH**

**Lüderitzer Weg 6**

**39517 Tangerhütte OT Brunkau**

- nachfolgend als Auftragnehmer bezeichnet -

und

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

- nachfolgend als Auftraggeber bezeichnet -

**Technische und organisatorische Maßnahmen**

1. **Maßnahmen zur Vertraulichkeit**
   1. **Beschreibung der Zutrittskontrolle:**

* Alarmanlage nach anerkanntem Standard
* Besucher bewegen sich nur in Begleitung in den Räumen, in denen Daten verarbeitet werden
* Chipkarten-/Transponder-Schließsystem
* Dokumentation der Schlüsselvergabe
* Elektronische Zutrittskontrolle oder Schließsysteme mit Chip oder Chipkarte
* Schließanlage
* Schlösser nach aktuellem Stand der Einbruchssicherheit
* Serverräume und Räume, in denen sich Daten befinden oder verarbeitet werden, sind abgeschlossen, wenn sich niemand darin befindet
* Türen und Fenster nach aktuellem Stand der Einbruchsicherheit
* Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile, zum Beispiel Nicht-Kennzeichnung des Serverraums
* Zutritt zu Räumen, in denen Daten aufbewahrt werden, die einer besonderen Geheimhaltung unterliegen (zum Beispiel gem. § 203 StGB), erhalten nur besonders berechtigte Personen
* Zutritt zu Räumen, in denen Daten gem. Art. 9 DSGVO aufbewahrt werden, erhalten nur besonders berechtigte Personen
* Zutritt zu schützenswerten Gebäudeteilen (zum Beispiel Serverraum) erhalten nur besonders berechtigte Personen
  1. **Beschreibung der Zugangskontrolle:**
* Authentifikation mit Benutzer + Passwort durch persönlichen und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
* Datenträger sind mit einem dem Stand der Technik entsprechenden Verfahren verschlüsselt
* Drucker, Kopierer und Multifunktionsgeräte sind so aufgestellt, dass nur befugte Benutzer hierzu Zutritt haben
* Externe Schnittstellen (z. B. USB-Ports) sind bei allen IT-Systemen, zu denen Dritte Zugang haben könnten, durch eine entsprechende Software gesperrt
* Intelligente Firewalls zum Schutz des Netzwerkes
* IT - Systeme sind so aufgestellt, dass nur befugte Benutzer die Bildschirminhalte einsehen können
* Mobile Device Management, d. h. zentralisierte Verwaltung von Mobilgeräten wie Smartphones, Notebooks, PDAs oder Tablets durch einen oder mehrere Administratoren mit Hilfe von Software und Hardware
* Mobile Geräte sind mit einem dem Stand der Technik entsprechenden Verfahren verschlüsselt
* Sorgfältige Auswahl und Zuverlässigkeitsprüfung von Hilfskräften (zum Beispiel Reinigungspersonal und Sicherheitspersonal)
* Sperrung der Clients bzw. Systeme nach gewissen Zeitintervallen ohne Useraktivität, auch durch passwortgeschützte Bildschirmschoner
* Verwaltung von Benutzerberechtigungen bei Eintritt, Änderung, Austritt
  1. **Beschreibung der Zugriffskontrolle:**
* Aktenvernichter der Sicherheitsstufe 3 und Schutzklasse 2 oder höher
* Clean-Desk-Prinzip, d. h. an unbeaufsichtigten Arbeitsplätzen besteht keine Zugriffsmöglichkeit auf sensible Informationen
* Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern durch Löschung der Zugriffsrechte, dokumentierte Rückgabe von Akten, Datenträgern, IT-Systemen und Mobilfunkgeräten
* Rollen- und Berechtigungskonzept mit Benutzergruppen, Benutzerprofilen und dazugehörigen Berechtigungen
* Rollenbasiertes Berechtigungskonzept für die Administratoren des Cloud-Diensteanbieters und für die Cloud-Benutzer des Cloud-Anwenders
* Sichere Aufbewahrung von Akten mit Daten besonderer Geheimhaltung, z. B. Mandanten- oder Patientenakten, in verschließbaren bzw. abgeschlossenen Stahl- oder Wertsicherungsschränken
* Sichere Aufbewahrung von Akten mit Daten gem. Art. 9 DSGVO, z. B. Personalakten, in verschließbaren bzw. abgeschlossenen Schränken
* Sichere Aufbewahrung von Datenträgern, z. B. USB-Sticks, CDs oder SD-Karten
* Sichere Löschung von Datenträgern vor deren Wiederverwendung durch Formatierung
* Technische Zugriffsbeschränkungen auf Drucker, Kopierer und Multifunktionsgeräte, z. B. durch Chipkarten oder PIN-Codes
* Verschlüsselung von Smartphones mit einem dem Stand der Technik entsprechenden Verfahren
* Vorgabe der Passwort-Parameter hinsichtlich Komplexität und Aktualisierungsintervall
  1. **Beschreibung der Weitergabekontrolle:**
* Datenschutztonnen und Entsorgung durch zertifizierte Dienstleister gemäß DIN 66399 oder Aktenvernichter der Sicherheitsstufe 3 oder höher
* Dokumentierte Verwaltung sämtlicher Datenträger mit laufender Bestandskontrolle
* Einheitliche E-Mail-Adressen mit einer Domain
* Nicht mehr benötigte Datenträger werden physikalisch zerstört
* SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
* Transportverschlüsselung von E-Mails, z. B. mittels TLS-Verfahren
* Verpackungs- und Versandvorschriften
* Verschlüsselung der Website nach SSL / HTTPS
* VPN-Tunnel zur Einwahl in das Firmen- Netzwerk von außen und bei der Internetnutzung
  1. **Beschreibung des Trennungsgebots:**
* Datentrennung auf Basis von Kunden- oder Mandantennummern
* Mandantenfähigkeit der IT-Systeme
* Technische Trennung von Entwicklungs-, Test- und Produktivsystem
  1. **Beschreibung der Pseudonymisierung:**
* Trennung von Kontaktdaten und anderen Daten
* Trennung von Kundenstammdaten und Auftragsdaten
  1. **Beschreibung der Verschlüsselung:**
* Cloud-Nutzung nur mit Verschlüsselung nach dem aktuellen Stand der Technik
* Datenbanken sind nach aktuellem Stand der Technik verschlüsselt
* Netzkommunikation nur mit Verschlüsselung nach dem aktuellen Stand der Technik
* Verschlüsselte Datenspeicherung, z. B. gem. AES256-Standard
* Verschlüsselte Datenübertragung, z. B. E-Mailverschlüsselung nach PGP oder S/Mime, Einsatz von VPN, verschlüsselte Internetverbindungen mittels TLS/SSL

1. **Maßnahmen zur Integrität**
   1. **Beschreibung der Eingabekontrolle:**

* Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen, nicht Benutzergruppen
* Nutzungsverbot nicht freigegebener Hard- und Software
* Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe
* Redundante Protokollierung der Eingabe, Änderung und Löschung von Daten

1. **Maßnahmen zur Verfügbarkeit und Belastbarkeit**
   1. **Beschreibung der Verfügbarkeitskontrolle:**

* Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
* Backup- / Recoverykonzept
* CO2 Feuerlöschgeräte in allen Serverräumen
* Durchführung einer Schwachstellenanalyse in den Bereichen Geländeschutz, Gebäudeschutz, Eindringen in Rechner, Eindringen in Netzwerke, Eindringen in Server
* Einhaltung von geltenden Brandschutz-Vorschriften
* Feuer- und Rauchmeldeanlagen
* Geräte zur Überwachung von Temperatur und Feuchtigkeit in allen Serverräumen
* Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft
* IT-Notfallpläne
* Klimaanlage in allen Serverräumen
* Professionelle Antivirensoftware zum Schutz vor Malware
* Professionelle Antivirensoftware zum Schutz vor Malware bei allen mobilen Geräten, wie Smartphones, Notebooks, Tablets
* Redundante Datenhaltung (z. B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum)
* Schutzsteckdosenleisten für alle IT-Systeme
* Überspannungsschutz für alle IT-Systeme
* Unterbrechungsfreie Stromversorgung für alle Server
* Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitten
* Vermeidung wasserführender Leitungen in allen Serverräumen
* Zutrittsbegrenzung in allen Serverräumen auf notwendiges Personal
  1. **Beschreibung der raschen Wiederherstellbarkeit:**
* Backup-Datenträger werden extern sicher aufbewahrt
* Backups der eingesetzten Software
* Durchführung regelmäßiger und dokumentierter Datenwiederherstellungen
* Durchführung regelmäßiger, mindestens täglicher Datensicherungen
* IT-Notfall- und Wiederanlaufpläne

1. **Weitere Maßnahmen zum Datenschutz**
   1. **Beschreibung der Auftragskontrolle:**

* Abschluss von Verträgen zur Auftragsverarbeitung gem. Art. 28 DSGVO
* Auftragnehmer eines AVV haben einen Datenschutzbeauftragten bestellt und benannt
* Auswahl der Auftragnehmer eines Auftragsverarbeitungsvertrages unter Sorgfaltsgesichtspunkten, insbesondere hinsichtlich Datensicherheit
* Laufende Überprüfung der Auftragnehmer, seiner Tätigkeiten sowie der Einhaltung des Vertrages
* Regelmäßige Audits mit dem Datenschutzbeauftragten der Auftragnehmer
* Schulung aller zugriffsberechtigten Mitarbeiter und regelmäßig stattfindende Nachschulungen
* Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO
  1. **Beschreibung des Managementsystems zum Datenschutz:**
* Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte werden nachvollziehbar dokumentiert
* Änderung und Ergänzungen von Verarbeitungstätigkeiten werden regelmäßig kontrolliert
* Betriebsanweisungen zur Einhaltung der Datenschutzrichtlinien
* Deaktivierungsmöglichkeit einzelner Funktionalitäten der IT-Systeme ohne Einfluss auf das Gesamtsystem
* Die Struktur der Daten und die Art der Speicherung sind so gestaltet, dass das Löschen der Inhalte einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten mit beherrschbarem Aufwandmöglich ist, ohne die Integrität des verbleibenden Datenbestandes und ohne besondere Zweckbindungsregelungen, z. B. von Protokolldaten, die der Datenschutzkontrolle dienen, zu beeinträchtigen.
* Dokumentation aller Verträge mit Kunden, Mitarbeitern, Kooperationspartnern, Auftragsverarbeitern und Gemeinsam Verantwortlichen, deren Daten erhoben, verarbeitet oder weitergeleitet werden oder die Daten erhalten
* Dokumentation von Einwilligungen und Widersprüchen
* Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verarbeitungstätigkeiten
* Dokumentierte Vertraulichkeitsverpflichtungserklärungen für alle Mitarbeiter und Kooperationspartner
* Einsatz notwendiger Datenfelder, z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
* Führung und Pflege eines umfassenden und detaillierten Verzeichnisses der technischen- und organisatorischen Maßnahmen
* Führung und Pflege eines umfassenden und detaillierten Verzeichnisses der Verarbeitungstätigkeiten
* Geregelte Einarbeitung von neuem Personal im Bereich der Informationssicherheit
* Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren; Bevorzugung von automatisierten Verarbeitungsprozessen
* Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen
* Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
* Permanentes Monitoring der Produktivsysteme zur Abwehr von Cyber-Attacken
* Reduzierung der Verarbeitungsoptionen durch Einsatz von Verarbeitungsprozessschritten, z. B. im CRM
* Reduzierung von erfassten Attributen der betroffenen Personen in der jeweiligen Verarbeitungstätigkeit
* Regelmäßige interne Audits
* Regelmäßige IT-Schwachstellenanalysen, z. B. Phishing- und/oder Penetrationstests
* Regelmäßige Prüfung der technischen und organisatorischen Maßnahmen mindestens einmal jährlich oder im Falle von wesentlichen Änderungen der Rahmenbedingungen
* Regelmäßige und dokumentierte Schulungen aller Mitarbeiter zum Datenschutz, mindestens einmal jährlich oder bei Änderungen der Rahmenbedingungen
* Regelmäßige Updates und Patches für alle IT-Systeme
* Richtlinie zur IT-Nutzung
* Schulungsprogramm zur IT-Sicherheit und Datenschutz
* Single Point of Contact (SPoC) für Betroffene und Datenschutzbehörden durch Einrichtung eines entsprechenden E-Mail-Postfaches
* Software mit datenschutzfreundlichen Voreinstellungen gem. Art. 25 Abs. 2 DSGVO
* Softwaregestützte Tools zur Einhaltung der datenschutzrechtlichen Anforderungen
* Spezielle Datenschutzrichtlinie für die Datenverarbeitung im Homeoffice
* Standardisierte Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Betroffenenrechten
* Störungen, Probleme und Änderungen an Verarbeitungstätigkeiten sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes werden nachvollziehbar dokumentiert
* Versionierung von Dateien zum Zweck der Nachverfolgbarkeit von Änderungen

**Anlage 3**

zum

**Auftragsverarbeitungsvertrag**

zwischen

**visuSolution GmbH**

**Lüderitzer Weg 6**

**39517 Tangerhütte OT Brunkau**

- nachfolgend als Auftragnehmer bezeichnet -

und

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

- nachfolgend als Auftraggeber bezeichnet -

**Personen mit Weisungsbefugnis**

* Die Geschäftsleitung des Auftraggebers oder von dieser namentlich bevollmächtigte Personen

**Personen/Dritte mit Kontrollrechten**

* Die Geschäftsleitung des Auftraggebers oder von dieser namentlich bevollmächtigte Personen