



Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

- nachstehend Auftraggeber –

und der

visuSolution GmbH
Lüderitzer Weg 6
39517 Tangerhütte

- nachstehend Auftragnehmer –

gemeinsam „Vertragsparteien“ genannt

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Diese Vereinbarung regelt die Rechte und Pflichten der Vertragsparteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Es gelten die Begriffsbestimmungen aus Art. 4 und Art. 9 DSGVO.

(3) „Auftragswartung“ meint hier die Leistungen des Auftragnehmers, bei deren Ausführung nicht auszuschließen ist, dass der Auftragnehmer Zugriff auf personenbezogenen Daten erhält, die der Auftraggeber verantwortet.

(4) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(5) „Unterauftragnehmer“ meint hier Dritte, die im Sinne des Art. 4 Nr. 10 DSGVO, die der Auftragnehmer mit schriftlicher Gestattung des Auftraggebers zur Leistungserbringung im Rahmen der „Wartungsverträge“ einsetzt.

2. Gegenstand der Vereinbarung

(1) Diese Vereinbarung tritt aufgrund ihrer rechtlichen Anforderungen zusätzlich zu ggf. bereits bestehenden „Wartungsverträgen“ in Kraft und konkretisiert bzw. ergänzt diese bereits bestehenden Verträge. Die Bestimmungen dieser Vereinbarung, einschließlich Ihrer Anlagen, gehen etwaigen widersprüchlichen Regelungen eines „Wartungsvertrages“ vor.

(2) Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

(3) Die vorliegende Vereinbarung beinhaltet die Regelungen zur Auftragsverarbeitung, die auf alle zwischen den Vertragsparteien geschlossenen Verträge anzuwenden sind. Verbindliche Vertragsbestandteile dieser Vereinbarung sind:

Anlage 1	Auftragsgegenstände
Anlage 2	Sicherheit der Datenverarbeitung
Anlage 3	Unterauftragnehmer
Anlage 4	Meldeformular für Datenschutzverstöße

3. Dauer der Auftragsverarbeitung

(1) Diese Vereinbarung tritt am Tag der Beauftragung in Kraft.

(2) Die Vereinbarung endet automatisch und ohne dass es einer Kündigung bedarf, wenn der Auftragnehmer für den Auftraggeber insgesamt keine Auftragsverarbeitung oder -wartung mehr betreibt.

(3) Das Recht zur außerordentlichen Kündigung aus wichtigem Grund nach Maßgabe des § 314 BGB bleibt unberührt.

(4) Der Auftraggeber kann einen Wartungsvertrag, ungeachtet etwaiger entgegenstehender Regelungen im Wartungsvertrag, kündigen, wenn der Auftragnehmer gegen eine gesetzliche Datenschutzbestimmung oder gegen eine Verpflichtung aus dieser Vereinbarung verstößt, oder eine Garantie verletzt. Die Kündigungsfrist beträgt in diesem Fall 3 Monate zum Monatsende. Ansprüche des Auftragnehmers wegen einer vorzeitigen Vertragsbeendigung, insbesondere Schadensersatz, sind ausgeschlossen.

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

5. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach dieser Vereinbarung und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen. Der Auftragnehmer bestätigt, die in seinem Verantwortungsbereich nach Art. 32 DSGVO erforderlichen Maßnahmen ergriffen zu haben. Die technischen und organisatorischen Maßnahmen sind in Anlage 2 zu dieser Vereinbarung aufgeführt.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(7) Der Auftragnehmer garantiert, dass er die bei ihm mit der Verarbeitung beschäftigten Personen zur Vertraulichkeit verpflichtet hat, und er diese Verpflichtung durch organisatorische Vorkehrungen auch nachhält. Die Verpflichtung der Vertraulichkeits- und Schutzbestimmungen gelten auch nach der Beendigung der Tätigkeiten.

6. Unterauftragnehmer

Der Auftragnehmer sichert die sorgfältige Auswahl von Unterauftragnehmern zu. Er sorgt dafür, dass beauftragte Unterauftragnehmer alle Bestimmungen dieser Vereinbarung und der einschlägigen gesetzlichen Bestimmungen der DSGVO ausführen.

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 3** zu diesem Vertrag angeben.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(3) Der Auftraggeber stimmt der in Anlage 3 abschließend aufgezählten Unterbeauftragung ausdrücklich zu.

(4) Etwaige Nachträge zur Unterbeauftragung sind schriftlich auszufertigen.

(5) Der Auftraggeber kann die Zustimmung zum Einsatz eines Unterauftragnehmers in begründeten Fällen, insbesondere im Fall einer Gesetzes- oder Pflichtverletzung, widerrufen. Der Auftragnehmer hat in diesem Fall unverzüglich die Unterbeauftragung der Verarbeitung einzustellen.

(6) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

7. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen (Anlage 4 zu dieser Vereinbarung).

(4) Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

8. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

9. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftrag-

geber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Sicherheit der Datenverarbeitung

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 2** zu diesem Vertrag beigefügt.

Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

13. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

(3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

14. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevanter Streitigkeit aus dem Leistungsvertrag ist Stendal. Gesetzliche Regelungen über ausschließende Zuständigkeiten bleiben unberührt.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____, den _____
Ort Datum

Auftraggeber


Tangerhütte, den 25.09.2018
Ort Datum
39517 Tangerhütte OT
Tel. +49 (0) 39 361 - 967 - 0
Fax: +49 (0) 39 361 - 96 43 90

Auftragnehmer

Anlage 1 „Auftragsgegenstand“ zur Vereinbarung der Auftragsverarbeitung nach Art. 28 DSGVO

1. Gegenstand der Auftragsverarbeitung

Durchführung einer Fernwartung, Support und Service für unsere Produkte auf den IT-Systemen des Auftraggebers.

2. Art und Zweck der Verarbeitung

Bei Nutzung der Videozentriertechnik werden notwendige Gesichtsbereiche (Nase, Augen, Ohren) bildverarbeitungstechnisch mit der visureal®Software erfasst und je nach System lokal oder extern gespeichert.

Das Kundenbild des Auftraggebers wird mit der Auswahl (Fassung, Glasart), Daten der Fehlsichtigkeit und den ermittelten Glasdaten eines Glasherstellers verknüpft.

Die daraus ermittelten Daten sind die Rezeptglasdaten, die zur Glasfertigung beim Glashersteller benötigt werden. Um die fehlerfreie Kommunikation der Systeme zu gewährleisten sind folgende Eingriffe möglich:

1. Ausführen von Installation/ Neuinstallationen
2. Prüfen der Einstellung von visuReal®
3. Prüfen der Kamerasäule samt Treiber/ AMCAP/ Stream Catcher
4. Fehleranalysen der visuReal®Software durch schrittweises nachvollziehen der Mess- und Eingabehistorie anhand von Kundendaten
5. Aktualisieren der Gerätetreiber per Fernwartung mittels TeamViewer- Software (auf Weisung des Auftraggebers).

3. Art der personenbezogenen Daten

Folgende Datenkategorien sind Gegenstand der Auftragsverarbeitung:

1. Personenstammdaten
2. Kommunikationsdaten (z.B. Telefon, E-Mail)
3. Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
4. Kundenhistorie
5. IP-Adresse
6. besondere Kategorien personenbezogener Daten (PD, HSA,, Kopfdrehung, -vorneigung)
7. Zugriffsrechte

4. Kategorien betroffener Personen

Folgende Kategorien von Betroffenen sind von der Auftragsverarbeitung betroffen:
Kunden des Auftraggebers

Anlage 2 „Sicherheit der Datenverarbeitung“ zur Vereinbarung der Auftragsverarbeitung nach Art. 28 DSGVO

Bei Fragen zur Informationssicherheit wenden Sie sich bitte an:

Kontakt:
visuSolution GmbH
Datenschutzbeauftragter
Lüderitzer Weg 3
39517 Tangerhütte

Tel. 039361/967-0
E-Mail: datenschutz@visusolution.com

technische und organisatorische Maßnahmen

Die von der visuSolution GmbH getätigten Datenschutzmaßnahmen haben das Ziel der dauerhaften Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit für zweckbestimmte Verwendung, sowie die Sicherstellung der Transparenz, Prüffähigkeit und bei Bedarf Intervention.

Die im Unternehmen getroffenen Maßnahmen gewährleisten, dass Unbefugte nicht auf Datenverarbeitungsanlagen Einfluss nehmen können, auf denen personenbezogenen Daten gespeichert sind:

Pseudonymisierung pers. Daten (Art. 32 Abs. 1 lit. a DSGVO)

Im Rahmen der Fernwartung speichert der Auftragnehmer keine Kundendaten des Auftraggebers auf seinen Systemen. Gespeichert werden lediglich Nutzungsdaten in Log-Files sowohl auf den Systemen des Auftraggebers, als auch auf denen des Auftragnehmers. Eine Pseudonymisierung im Rahmen der Fernwartung ist somit nicht vorgesehen. Ist es notwendig, Kundendatenbanken an den Auftragnehmer zu übermitteln, so wird der Auftraggeber entsprechende Weisungen erteilen.

Verschlüsselung pers. Daten (Art. 32 Abs. 1 lit. a DSGVO)

Die Fernwartung unterliegt der Sicherheitstechnik des Teamviewers.
<https://www.teamviewer.com/de/security/>

Maßnahmen zur Sicherstellung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Der Auftragnehmer sichert dem Auftraggeber zu, dass Unbefugten durch folgende Maßnahmen der Zutritt und Zugang zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet oder gespeichert werden:

- Zutritt zu den Büroräumen nur durch oder in Begleitung von berechtigten Personen
- zentrale Zutrittsregelung (z. Bsp. verschlossene Haupteingangstür)
- dokumentierte Schlüsselausgabe an ausgewählte Mitarbeiter
- Lagerung von vertraulichen Unterlagen in abschließbaren Schränken bzw. im Tresor
- Sicherung des Gebäudes durch eine Alarmanlage

Der Auftragnehmer sichert darüber hinaus zu, dass Unbefugte durch folgende Maßnahmen an der Benutzung der Datenverarbeitungssysteme gehindert werden:

- IP-beschränkte Zugriffe auf den Server
- Benutzerprofil pro User
- Berechtigungskonzept für digitale Zugriffsmöglichkeiten
- Persönlicher und individueller User-Log-In bei Anmeldung am System
- Nutzerbezogene komplexe Passwörter
- Automatische Sperrung unserer IT-Systeme bei Nichtbenutzung.

Die im Unternehmen getroffenen Maßnahmen zur Vertraulichkeit und Integrität gewährleisten, dass die Benutzung eines Datenverarbeitungssystems ausschließlich von den Berechtigten erfolgen kann. Darüber hinaus wird sichergestellt, dass personenbezogenen Daten bei der Verarbeitung, Nutzung und Speicherung nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können:

- differenzierte und aufgabenbezogene Berechtigungsprofile
- Verpflichtung aller Mitarbeiter auf das Datenschutzgeheimnis

Maßnahmen zur Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Der Auftragnehmer hat Maßnahmen getroffen, die eine Weitergabekontrolle gewährleisten, damit bei der elektronischen Übertragung oder während des Transports Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- VPN Tunnel zur Datenübertragung, der mit Benutzerkonto und Passwort gesichert ist
- Festplatten und Notebooks sind grundsätzlich mit geeigneten Maßnahmen zu verschlüsseln
- existierende Regelungen zur Datenvernichtung und Löschung
- die Fernwartung unterliegt der Sicherheitstechnik des Teamviewers
- sonstige Übertragungen und Übermittlungen erfolgen ausschließlich auf Weisung des Auftraggebers.

Die im Unternehmen getroffenen Maßnahmen zur Integrität der Daten gewährleisten eine hinreichend Eingabekontrolle:

- Protokollierung in Log-Files
- Log-Files werden stichprobenartig geprüft
- Benutzername, Datum und Uhrzeit der Anmeldung wird automatisch bei Veränderung gespeichert.

Die im Unternehmen getroffenen Maßnahmen der Trennungskontrolle gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- mandantenfähige Software
- Entwicklungs- und Testsysteme werden ausschließlich mit Testdaten betrieben.

Maßnahmen zur Sicherstellung der Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Die getroffenen Maßnahmen zur Verfügbarkeitskontrolle gewährleisten, dass personenbezogene Daten gegen zufällig Zerstörung oder Verlust geschützt sind:

- regelmäßiges Backup Verfahren
- USV (Universelle Stromversorgung)
- Virens Scanner AVAST Professional auf allen Clients und Server, automatische Aktualisierung-Server gesteuert
- Hard- und Softwarefirewall
- Brandmeldeanlage
- Alarmanlage und Wachschutzsicherung.

Das Schutzniveau in Bezug auf die Auftragskontrolle wird durch folgende Maßnahmen gewährleistet:

Maßnahmen zur Wiederherstellung, der Verfügbarkeit und dem Zugang zu pers. Daten bei einem technischen Zwischenfall (Art. 32 lit. c DSGVO)

Regelmäßige Backups im Rahmen eines Notfallkonzeptes vorhanden.

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

Es existiert ein Datenschutzkonzept im Rahmen einer unternehmensinternen Datenschutzrichtlinie.

Die visuSolution GmbH beauftragt nur Dienstleister unter Berücksichtigung der Vorgaben der DSGVO und des BDSG, insbesondere gem. Artikel 28 Abs. 3 DSGVO oder einer vergleichbaren Garantie.

Anlage 3 „Unterauftragnehmer“ zur Vereinbarung der Auftragsverarbeitung nach Art. 28 DSGVO

Folgende Unterauftragnehmer sind mit Zustimmung des Auftraggebers tätig:

<p>Unterauftragnehmer:</p>	<p>Ollendorf Mess-Systeme Dipl. Ing. Hans-Joachim Ollendorf Zur Springe 5 in 39517 Tangerhütte</p> <p>Entwickler (Hardware/ Software) Softwareentwickler und Lizenzgeber</p>
<p>Unterauftragnehmer der Firma Ollendorf Mess-Systeme (Auftragnehmer der Ollendorf Mess-Systeme gem. Art. 28 Abs. 3 DSGVO)</p>	<p>Amazon Web Services https://aws.amazon.com/de/compliance/eu-data-protection/ https://aws.amazon.com/de/data-protection/</p> <p>Hosting und Bereitstellung der Funktionsumgebung</p> <p>UCDplus GmbH Geißlerstraße 3 in 39104 Magdeburg</p> <p>Programmierung, Wartung und Pflege</p>
<p>Unterauftragnehmer der Firma UCDplus GmbH (Auftragnehmer der UCD+ GmbH gem. Art. 28 Abs. 3 DSGVO)</p>	<p>Webvariants GmbH & Co. KG Liebigstraße 7 in 39104 Magdeburg</p> <p>Programmierung, Wartung und Pflege</p> <p>KF Interactive GmbH Fockerstraße 6 in 04275 Leipzig</p> <p>Programmierung, Wartung und Pflege</p> <p>pixonauten Tristan Feldbusch Buchenweg 2 in 39167 Irxleben</p> <p>Programmierung, Wartung und Pflege</p>

Anlage 4 „Meldeformular für Datenschutzverstöße“ zur Vereinbarung der Auftragsverarbeitung nach Art. 28 DSGVO

Auftragnehmer (Name, Anschrift): visuSolution GmbH, Lüderitzer Weg 6
39517 Tangerhütte

Auftraggeber (Name, Anschrift):

Nähere Bezeichnung des betroffenen Auftragsverhältnisses:

Zeitraum des Vorfalles (Datum, Uhrzeit):	
Beschreibung des Datenschutzvorfalls (Verletzung des Schutzes personenbezogener Daten)	
Betroffene personenbezogene Daten (nach Datenkategorien)	
Zahl der betroffenen Personen (ungefähr)	
Zahl der betroffenen Datensätze (ungefähr)	
betroffene IT-Systeme:	
zuständiger Fachbereich / ggf. zuständige IT-Abteilung	
Name und Kontaktdaten des Datenschutzbeauftragten oder sonstiger Anlaufstelle	
Verfasser und Datum der Meldung:	
Wer wurde bereits durch wen informiert (z.B. Datenschutzbeauftragter, Datenschutz-Aufsichtsbehörde etc.)	
davon erfahren durch (Quelle):	

Beschreibung der wahrscheinlichen Folgen des Datenschutzvorfalls	
Beschreibung der vom Auftragnehmer ergriffenen Sofortmaßnahmen zur Behebung	
Vorschlag für zu ergreifende Maßnahmen	
Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen	
Gesamtrisiko:	

Rechtsverbindliche Bestätigung der Richtig- und Vollständigkeit vorstehender Angaben:

Datum

Datum

Unternehmensleitung

ggf. Datenschutzbeauftragter