Vereinbarung

über eine

Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem/der

.....

- als Verantwortlicher - nachstehend „Auftraggeber“ genannt -

und

Wohlstreicher Software, Indlinger Str. 8b, 94060 Pocking

- als Auftragsverarbeiter - nachstehend „Auftragnehmer“ genannt

Inhaltsverzeichnis

1. Management Summary

Dieses Dokument regelt die Rechte und Pflichten von Verantwortlichen und Auftragsverarbeiter (in Folge auch „Auftragnehmer“ genannt) in Bezug auf die Vereinbarung über die Auftragsverarbeitung personenbezogener Daten. Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragsverarbeiters oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Verantwortlichen verarbeiten.
In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Durchführung von Wartungsarbeiten zur Anpassung, Hilfestellung oder Korrektur der vom Auftragnehmer gelieferten Software.

(2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 6 Monaten zum Jahresende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

3. Konkretisierung des Auftragsinhalts

(1) **Art und Zweck der vorgesehenen Verarbeitung von Daten**

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Anpassung, Hilfestellung oder Korrektur der Software in Hinblick auf Fragen, Änderungswünsche oder Reklamation des Auftraggebers.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44, sowie Art 45. Abs. 1 DS-GVO erfüllt sind.

(2) **Art der Daten**

Folgende Datenkategorien werden verarbeitet:

Kontaktdaten, Vertragsdaten , Verrechnungsdaten, Bestelldaten, Entgeltdaten

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

Kunden, Interessenten , Lieferanten, Ansprechpartner, Beschäftigte, Dienstleister, Auftragsverarbeiter

4. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikations- leistungen, Post-/Transpordienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit

der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der „Anlage 1“ zu diesem Vertrag angeben.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Der Auftragnehmer ist nach Art. 28 Abs. 4 DSGVO verpflichtet, gegenüber Subunternehmern dieselben Pflichten wie in diesem Auftragsverarbeitungsvertrag zu vereinbaren.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Daten des Auftraggebers ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers zu dem in diesem Vertrag festgelegten Zwecken und Umfang und verarbeitet die Auftraggeber-Daten nicht für eigene Zwecke.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(4) Der Auftragsgeber übt sein Weisungsrecht in Bezug auf die Daten entsprechend durch Konfiguration, Einrichtung und Benutzung der eigenen Hotel- und Gästeverwaltungssoftware (PMS, CRS, CRM etc.) aus. Durch die Steuerung der eigenen Hotel- und Gäste-verwaltungssoftware erteilt der Auftraggeber z.B. Weisungen in Bezug auf die Eingabe, Speicherung, Korrektur, Übersendung, Auswertung und Löschung der Buchungs- und Gästeinformationen.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(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.

(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.

13. Haftung

Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Verantwortlicher und Auftragsverarbeiter als Gesamtschuldner.

Der Auftragsverarbeiter trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragsverarbeiter den Verantwortlichen auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Verantwortlichen erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragsverarbeiter dem Verantwortlichen ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

Der Auftragsverarbeiter haftet dem Verantwortlichen für Schäden, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Verantwortlichen erteilten Weisung entstanden ist.

Folgende Anlagen zu diesem Vertrag sind Bestandteil desselben:

Anlage 1 – Unterauftragsverhältnisse

Anlage 2 – Technisch-organisatorische Maßnahmen

_____	Pocking, den 17.05.2018_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anlage 1 – Unterauftragsverhältnisse

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“). Änderungen bzw. Ergänzungen werden per E-Mail bekannt gegeben.

Dabei handelt es sich um nachfolgende Unternehmen:

Strato AG

Pascalstraße 10

10587 Berlin

Anlage 2 – Technisch-organisatorische Maßnahmen

Wahrung der Vertraulichkeit personenbezogener Daten

• Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch räumlich abgesicherte Server, zu denen nur Befugte Zutritt erhalten

• Zugangskontrolle

Keine unbefugte Systembenutzung, durch sichere Kennwörter, automatische Sperrmechanismen und Einsatz geeigneter Sicherheitssoftware (Virenschutz, Firewall)

• Zugriffskontrolle

Einsatz von Berechtigungskonzepten und bedarfsgerechte Zugriffsrechte mit entsprechenden Passwortrichtlinien. Akten werden ordnungsgemäß nach Ablauf der Aufbewahrungsfrist vernichtet.

• Trennungskontrolle

Daten werden dem Verarbeitungszweck gemäß getrennt aufbewahrt auf unterschiedlichen Servern. Datenbankrechte sind limitiert und zweckgemäß vergeben und bei Bedarf pseudonymisiert.

Wahrung der Integrität personenbezogener Daten

• Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

• Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch Protokollierung der Zugriffe und Rechtevergabe.

Wahrung der Verfügbarkeit personenbezogener Daten

• Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Strategien, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne. Für eine rasche Wiederherstellbarkeit im Falle wird gesorgt.

• Auftragskontrolle

Auftragnehmer, die Daten im Auftrag verarbeiten, werden sorgfältig geprüft. AV-Verträge mit Auftragnehmern werden geschlossen.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Interne Kontrolle der Verfahren, Richtlinien und Konzepte zur Gewährung der Datensicherheit