Vereinbarung

über die

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
Name Kunde	**MS IT Consulting GmbH**
Anschrift Kunde	5020 Salzburg, Innsbrucker Bundesstraße 126
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieses Auftrages ist die Verarbeitung von Eigen- und Fremddaten zur Bereitstellung der Online-Registrierkassenlösung „Q-Bon“. Diese Vereinbarung ist als Ergänzung zu dem bereits vom Auftraggeber erteilten Auftrag gegenüber der Auftragnehmerin zu verstehen. Die Einzelheiten der Leistungen ergeben sich aus den Allgemeinen Geschäftsbedingungen (https://www.q-bon.at/pdf/agbs.pdf), welche bei der Registrierung vom Auftraggeber akzeptiert werden. Auf diese Leistungen wird hier verwiesen.

(2) Es werden sämtliche Datenkategorien verarbeitet, welche zur Erfüllung der beauftragten Aufgaben zweckmäßig erscheinen, insbesondere: Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Transaktionsdaten, Geschäftsdaten, Bonitätsdaten, Bestelldaten und Entgeltdaten.

(3) Umfang, Art und Zweck der Datenverarbeitung ergeben sich aus der Nutzung der Online-Registrierkassenlösung „Q-Bon“. Im Übrigen ergeben sich Umfang, Art und Zweck der Verarbeitung personenbezogener Daten auch ausreichend aus der Leistungsvereinbarung.

(4) Gegenstand der Verarbeitung sind personenbezogene Kundendaten des Auftraggebers. Die durch die Verarbeitung ihrer personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen sind: Auftraggeber, Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte, Behörden, sonstige sich im Sphärenbereich des Auftraggebers befindliche Dritte.

2. DAUER DER VEREINBARUNG

Die Laufzeit des vorliegenden Vertrages richtet sich nach der Leistungsvereinbarung und den dortigen Kündigungsfristen. Eventuell bestehende Verträge zur Auftragsdatenverarbeitung werden durch den Abschluss des vorliegenden Vertrages ersetzt.

3. TECHNISCH-ORGANISATORISCHE MASSNAHMEN

Die Umsetzung der in der Anlage 1 dargelegten „Technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO“ durch den Auftragnehmer vor Beginn der Verarbeitung wird in einem IT-Sicherheitskonzept dokumentiert, das der Auftraggeber auf Anfrage einsehen kann. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Die Dokumentation des IT-Sicherheitskonzeptes enthält Darlegungen zu allen gemäß Art. 32 DSGVO notwendigen Maßnahmen nach den allgemein anerkannten Schutzzielen der IT-Sicherheit, insbesondere der Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit usw. Dabei wird ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau beachtet.

Die Verarbeitung von Daten in Privatwohnungen ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet, soweit damit das dauerhafte physische Vorhalten von Daten des Auftraggebers auf Datenträgern in der Privatwohnung verbunden ist. Zulässig ist jedoch die temporäre Zwischenspeicherung durch den Einsatz von mobilen Geräten (z.B. Laptops, Tablet-PCs, Smartphones etc.), sofern die mobilen Geräte über ausreichende, den anerkannten Standards entsprechende Sicherungseinrichtungen (z.B. VPN-Anbindung, Festplattenverschlüsselung etc.) verfügen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung, so dass es dem Auftragnehmer gestattet ist, adäquate Alternativmaßnahmen umzusetzen. Dabei wird das Sicherheitsniveau der festgelegten Maßnahmen insgesamt nicht unterschritten. Wesentliche Änderungen sind zu dokumentieren.

4. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht der Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber auf dessen Wunsch hin zu übergeben oder in dessen Auftrag zu vernichten. Dies unter der Voraussetzung, dass keine offenen Honoraransprüche des Auftragnehmers vorliegen.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstoße gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

5. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

6. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer kann Sub-Auftragsverarbeiter im Rahmen der Leistungsvereinbarung und des erteilten Auftrages hinzuziehen.

Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

7. KONTROLLRECHTE DES AUFTRAGGEBERS

Der Auftraggeber hat das Recht, eine angemessene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen. Er hat das Recht, sich durch rechtzeitig vorher anzumeldende Kontrollen, von der Einhaltung dieser Vereinbarung, auch im Geschäftsbetrieb des Auftragnehmers, zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Unterlagen verfügbar zu machen.

8. MITTEILUNG BEI VERSTÖSSEN DES AUFTRAGNEHMERS

Der Auftragnehmer erstattet dem Auftraggeber Meldung, wenn Verstöße gegen Datenschutzvorschriften oder vertragliche Vereinbarungen, die dem Schutz der personenbezogenen Daten des Auftraggebers dienen, vorgefallen sind.

Dem Auftragnehmer ist bekannt, dass der Auftraggeber nach Art. 33, 34 DSGVO verpflichtet ist, Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und unverzüglich, möglichst binnen 72 Stunden den Aufsichtsbehörden bzw. im Falle hoher Risiken der betroffenen Person zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragnehmer den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem Auftraggeber ohne Ansehen der Verursachung unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- eine Beschreibung der Art der Verletzung, der Kategorien und ungefähren Anzahl der betroffenen Personen und personenbezogenen Datensätze,
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung,
- eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Art. 33, 34 DSGVO treffen, wird der Auftragnehmer ihn hierbei unterstützen.

9. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

Der Umgang mit den personenbezogenen Daten erfolgt im Rahmen der getroffenen Vereinbarungen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers erteilen.

Die Datenverarbeitung erfolgt nur durch Auftrag des Auftraggebers, es sei denn, der Auftragnehmer ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung dieser Daten verpflichtet (z.B. bei Ermittlungen von Strafverfolgungs- oder

Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht untersagt.

Der Auftragnehmer verwendet die Daten nur für die vereinbarten Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Vertragsdurchführung oder die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, ein Auftrag verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch einen Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. LÖSCHUNG VON DATEN UND RÜCKGABE VON DATENTRÄGERN

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche eventuell noch in seinem Besitz befindlichen personenbezogenen Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, soweit die Daten nicht dem Nachweis der auftrags- und ordnungsgemäßen Leistungserbringung oder gesetzlichen Aufbewahrungspflichten unterliegen.

[*Ort*], am [*Datum*]	Salzburg, am [*Datum*]
Für den Auftraggeber:	*Für den Auftragnehmer:*
.....	.....
Name Klient	**MS IT Consulting GmbH**

Anlage 1

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Sicherheitsmaßnahmen)

Präventive Sicherheitsmaßnahmen – Maßnahmen zur Verhinderung eines erfolgreichen Angriffs

- Technische Maßnahmen
  - **Logische Zugriffskontrolle**: Die Vergabe von Zugriffsberechtigungen erfolgt nach dem „Need-to-Know"-Prinzip.
  - **Authentifizierung**: Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung.
  - **Passwortsicherheit**: Soweit Passwörter zur Authentifizierung eingesetzt werden, sollten diese mindestens 8 Zeichen lang sein und aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen bestehen. Passwörter werden ausschließlich verschlüsselt gespeichert.
  - **Verschlüsselung auf dem Übertragungsweg**: Personenbezogener Daten werden auf dem Übertragungsweg über das Internet verschlüsselt.
  - **Netzwerksicherheit**: Es wird eine Firewall eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit möglich – eingehenden Netzwerkverkehr blockiert.
  - **Maßnahmen gegen Schadsoftware**: Es wird nach Möglichkeit auf allen Systemen Anti-Viren Software eingesetzt. Alle eingehenden E-Mails werden automatisch auf Schadsoftware gescannt.
  - **Management von Sicherheitslücken**: Soweit möglich, wird auf allen Geräten die automatische Installation von Sicherheitsupdates aktiviert. Ansonsten erfolgt die Installation kritischer Sicherheitsupdates binnen 3 Arbeitstagen, die Installation von Sicherheitsupdates mittlerer Kritikalität binnen 25 Arbeitstagen und die Installation von Sicherheitsupdates geringer Kritikalität binnen 40 Arbeitstagen.

- Organisatorische Maßnahmen
  - **Klare Zuständigkeiten**: Interne Zuständigkeiten für Fragen der Datensicherheit werden definiert.
  - **Verschwiegenheitspflicht der Dienstnehmer**: Die Dienstnehmer werden über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere werden sie dazu verpflichtet, personenbezogene Daten nur auf ausdrückliche Anweisung eines Vorgesetzten an Dritte zu übermitteln.
  - **Schulungen und Informationsmaßnahmen**: Die Dienstnehmer werden zu Fragen der Datensicherheit (intern oder extern) geschult und angemessen über Fragen der Datensicherheit informiert (z.B. Passwortsicherheit).
  - **Geordnete Beendigung des Dienstverhältnisses**: Bei Beendigung des Dienstverhältnisses erfolgt eine unverzügliche Sperrung aller Konten des ausscheidenden Dienstnehmers sowie eine Abnahme aller Schlüssel des ausscheidenden Dienstnehmers.

- **Verwaltung von Computer-Hardware**: Es werden Aufzeichnungen darüber geführt, welchem Mitarbeiter welche Endgeräte (z.B. PC, Laptop, Mobiltelefon) zugewiesen wurden.
- **Eingabekontrolle**: Es bestehen Verfahren zur Kontrolle der Richtigkeit der eingegebenen personenbezogenen Daten.
- **Keine Doppelverwendung von Benutzer-Accounts**: Jede Person sollte ihren eigenen Benutzer-Account haben. Das Teilen von Benutzer-Accounts ist untersagt.
- **Keine unnötige Verwendung administrativer Accounts**: Benutzer-Accounts mit administrativen Rechten werden nur in Ausnahmefällen verwendet. Die reguläre Nutzung von IT-Systemen erfolgt ohne administrative Rechte.
- **Auswahl der Dienstleister**: Bei der Auswahl von Dienstleistern wird das vom Dienstleister gebotene Datensicherheitsniveau berücksichtigt. Der Einsatz eines Dienstleisters, der als Auftragsverarbeiter einzustufen ist, erfolgt nur nach Abschluss einer Auftragsverarbeitervereinbarung.
- **Sichere Datenentsorgung**: Papier, welches personenbezogene Daten enthält, wird grundsätzlich geschreddert bzw. einem externen Dienstleister zur sicheren Vernichtung übergeben. Datenträger werden vor ihrer Entsorgung vollständig überschrieben oder physisch zerstört, sodass die darauf gespeicherten Daten nicht wiederhergestellt werden können.

– Physische Maßnahmen

- **physische Zugangskontrolle**: Das Betreten der Betriebsräumlichkeiten ist für betriebsfremde Personen nur in Begleitung einer betriebsangehörigen Person zulässig.
- **Einbruchssicherheit**: Die Zugänge zu den Betriebsräumlichkeiten verfügen über einen angemessenen Einbruchsschutz (z.B. eine Sicherheitstüre höherer Widerstandsklasse, Alarmanlage).
- **Schlüsselverwaltung**: Schlüssel, welchen den Zugang zu den Betriebsräumlichkeiten oder Teilen derselben ermöglichen, werden nur an besonders vertrauenswürdige Personen ausgehändigt und dies auch nur soweit und solange diese Personen tatsächlich einen eigenen Schlüssel benötigen.

Detektive Sicherheitsmaßnahmen – Maßnahmen zur Erkennung eines Angriffs

- Technische Maßnahmen
  - **Scans nach Schadsoftware**: Es werden regelmäßig Scans nach Schadsoftware (Anti-Viren-Scans) durchgeführt, um Schadsoftware zu identifizieren, welche ein IT-System bereits kompromittiert hat.
  - **Automatische Prüfung von Logfiles**: Soweit die Sicherheits-Logfiles mehrerer System auf einem System zentralisiert gesammelt werden, erfolgt eine automatisierte Auswertung der Logfiles, um mögliche Sicherheitsverletzungen zu erkennen.
  - **Sicherheits-Mailing-Listen**: Es wird sichergestellt, dass ein Mitarbeiter des Unternehmens oder ein externer Dienstleister einschlägige Mailing-Listen für die Bekanntgabe neuer IT-Sicherheits-Bedrohungen abonniert (z.B. Mailing-Listen der Hersteller der verwendeten Software), um über die aktuelle Bedrohungslage in Kenntnis zu sein.

- Organisatorische Maßnahmen
  - **Erkennung von Sicherheitsverletzungen durch Dienstnehmer**: Alle Dienstnehmer werden instruiert, wie sie Sicherheitsverletzung erkennen können (z.B. nicht mehr auffindbare Computer-Hardware, Meldungen von Anti-Viren-Software).
  - **Betriebsfremde Personen**: Alle Dienstnehmer werden instruiert, betriebsfremde Personen anzusprechen, sollten sie in den Betriebsräumlichkeiten angetroffen werden.
  - **Audits**: Es werden regelmäßige Audits durchgeführt (z.B. Prüfung, ob alle kritischen Sicherheits-Updates installiert wurden).
  - **Manuelle Prüfung von Logfiles**: Soweit Logfiles geführt werden (z.B. über erfolglose Authentifizierungsversuche), werden diese in regelmäßigen Abständen geprüft.

- Physische Maßnahmen
  - **Brandmelder**: In den Betriebsräumlichkeiten ist ein Brandmelder installiert, der durch Rauch automatisch ausgelöst wird.

Reaktive Sicherheitsmaßnahmen – Maßnahmen zur Reaktion auf einen Angriff

- Technische Maßnahmen
  - **Datensicherung**: Es werden regelmäßig Datensicherungen erstellt und sicher aufbewahrt.
  - **Datenwiederherstellungskonzept**: Es wird ein Konzept zur raschen Wiederherstellung von Datensicherungen entwickelt, um nach einer Sicherheitsverletzung zeitnah den regulären Betrieb wieder herstellen zu können.
  - **Automatische Entfernung von Schadsoftware**: Die eingesetzte Anti-Viren-Software verfügt über die Funktion, Schadsoftware automatische zu entfernen.

- Organisatorische Maßnahmen
  - **Meldepflicht für Dienstnehmer**: Alle Dienstnehmer werden angewiesen, Sicherheitsverletzungen unverzüglich an eine zuvor definierte interne Stelle bzw. Person zu melden.
  - **Meldepflicht für externe Dienstleister**: Allen Dienstleistern wurden Kontaktdaten für die Meldung von Sicherheitsverletzungen mitgeteilt.
  - **Prozess für die Reaktion auf Sicherheitsverletzungen**: Es wird durch einen geeigneten Prozess sichergestellt, dass Sicherheitsverletzungen innerhalb von 72 Stunden ab Kenntnis von der Sicherheitsverletzung an die Datenschutzbehörde gemeldet werden können. Insbesondere sind allen Dienstnehmern die Notfall-Telefonnummern der zu involvierenden Personen bekannt zu geben (z.B. Notfall-Telefonnummer für den IT-Support).

- Physische Maßnahmen
  - **Feuerlöscher**: In den Betriebsräumlichkeiten gibt es eine geeignete Anzahl an Feuerlöschern. Allen Dienstnehmern ist bekannt, wo sich die Feuerlöscher befinden.
  - **Feueralarm**: Es sind Brandmelder installiert, die über eine automatische Verbindung zur Feuerwehr verfügten.

Abschreckende Sicherheitsmaßnahmen – Maßnahmen zur Minderung der Angreifermotivation

- Technische Maßnahmen
  - **Automatische Warnmeldungen**: Nutzer erhalten automatische Warnmeldungen bei risikoträchtiger IT-Nutzung (z.B. durch den Webbrowser, wenn eine verschlüsselte Website kein korrektes SSL/TLS-Zertifikat verwendet).

- Organisatorische Maßnahmen
  - **Sanktionen bei Angriffen durch eigene Dienstnehmer**: Alle Dienstnehmer werden darüber informiert, dass Angriffe auf betriebseigene IT-Systeme nicht toleriert werden und schwerwiegende arbeitsrechtliche Konsequenzen, wie insbesondere eine Entlassung nach sich ziehen können.