

Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

Der Auftragsverarbeiter:

Nutzer von helloCash

helloCash betrieben durch mRaP GmbH
Pulvermühlweg 11, 3250 Wieselburg,
Österreich

(im Folgenden Auftraggeber)

(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

- (1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: Erfüllung der Aufgaben aus dem Vertragsverhältnis zu helloCash:
- a. Registrierkasse
 - b. Rechnungserstellung
 - c. Mitarbeiterverwaltung
 - d. Kundenverwaltung
 - e. Angebotsverwaltung
 - f. Lieferscheine
 - g. Online-Buchung
 - h. Verrechnung

Diese Vereinbarung ist als Ergänzung zu den Allgemeinen Geschäftsbedingungen und Datenschutzbestimmungen zu sehen.

- (2) Folgende Datenkategorien werden verarbeitet:
- a. Unternehmensdaten
 - b. Artikeldaten
 - c. Dienstleistungsdaten
 - d. Administrationsdaten
 - e. Kassendaten
 - f. Kundendaten
 - g. Buchungsdaten
 - h. Logfiles
 - i. Mitarbeiterdaten
 - j. Rechnungsdaten
 - k. Angebotsdaten
 - l. Lieferscheindaten

- (3) Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung:
- a. Interessenten
 - b. Kunden

- c. Lieferanten
- d. Ansprechpartner
- e. Mitarbeiter

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann gemäß der AGBs von helloCash gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. PFLICHTEN DES AUFTRAGNEHMERS

- (1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen 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. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.
- (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 (Einzelheiten sind der Anlage./1 zu entnehmen).
- (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 jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, 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 zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
- (9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in den USA (z.B.: Google). Das angemessene Datenschutzniveau ergibt sich aus

- verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.

5. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer kann Sub-Auftragsverarbeiter hinzuziehen. Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. 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 eingetht, 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.

6. SONSTIGES

(1) Die Unwirksamkeit einer Bestimmung dieser Vereinbarung berührt die Gültigkeit der übrigen Bestimmungen nicht. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

(2) Sämtliche Vereinbarungen, die eine Änderung, Ergänzung oder Konkretisierung dieser Vereinbarung beinhalten, sowie besondere Zusicherungen und Abmachungen oder eine Änderung dieser Regel selbst sind schriftlich oder elektronisch niederzulegen.

(3) Es gilt das Recht der Österreichischen Republik.

(4) Dieser ADVV tritt per 24.5.2018 in Kraft.

(5) Eine Änderung wird mindestens 2 Wochen vor der Änderung per Email kommuniziert.

[Ort], am [Datum]

Wieselburg, am 26.4.2018

Für den Auftraggeber:

Für den Auftragnehmer:

.....
[Name samt Funktion]

mRaP GmbH
Pulvermühlweg 11
3250 Wieselburg

.....
Mag. Laurenz Gröbner, Geschäftsführung

Anlage ./1 - Technisch-organisatorische Maßnahmen

VERTRAULICHKEIT

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle:** Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

INTEGRITÄT

- **Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- **Rasche Wiederherstellbarkeit**, vorausgesetzt der technischen Möglichkeit.
- **Löschungsfristen:** Die Löschungsfristen betragen grundsätzlich 30 Jahre.

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Datenschutzfreundliche Voreinstellungen;
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers