Riecken Webservice & Application GmbH
Kaiserstr. 10
A – 1070 Wien

E office@riecken-webservices.at
T +43 1 375 00 51

EU-Datenschutz-Grundverordnung (DSGVO)

Vereinbarung über eine Auftragsdatenverarbeitung nach Art 28 DSGVO

zwischen der

Riecken Webservice & Application GmbH

FN 412181z

Kaiserstraße 10

1070 Wien

- nachstehend Dienstleister genannt -

und

- nachstehend Auftraggeber genannt -

Riecken Webservice & Application GmbH
Kaiserstr. 10
A – 1070 Wien

E office@riecken-webservices.at
T +43 1 375 00 51

Am heutigen Tage wie folgt:

I. Gegenstand der Dienstleistung

(1) Der Dienstleister erbringt für den Auftraggeber folgende Leistungen

Die DebitorCloud erstellt für den Anwender diverse Auswertungen bzw. Reports seiner OPOS Bestände. Zusätzlich werden die OPOS Bestände ausgewertet und die diversen Debitorenkennzahlen auf diverse Art und Weise (z.B. in Graphen, PDF Reports, Listen) dargestellt. Zusätzlich werden zum Vergleich externe Branchenkennwerte dargestellt, die dem Vergleich der Kundenbezogenen Werte zu den Branchenwerten dienen sollen. Ebenso wird Kundenkommunikation über das System abgewickelt. Die DebitorCloud versendet transparent E-Mails mit den Mahnungsreports als PDF im Anhang an die entsprechenden Kunden. Diese Kundenkommunikation inkl. Der erstellten Reports bzw. Anhänge werden im System angehängt. Das Einbringen von Drittanhängen ist möglich. Die DebitorCloud ermöglicht es in der Liste mit diversen Möglichkeiten zu Filtern und automatische Aktionen in regelmäßigen Abständen auf diese Filter auszuführen. Die DebitorCloud bezieht sich hierbei auf Kunden OP, sowie die Kundenstammdaten, als auch die Sachkontenbeschriftungen. Die Reaktion der Kunden auf die gesendete Kundenkommunikation wird analysiert. Die gesamten analysierten Werte sollen dem Unternehmer eine Unterstützung bieten, das Forderungsmanagement zu überwachen und zu verbessern und damit seine Liquidität zu verbessern. Zudem soll das gesamte Forderungsmanagement deutlich automatisierter und effizienter werden.

(2) Dazu stellt der Auftraggeber bzw. dessen Mandant dem Dienstleister folgende Daten bereit:

OPOS Liste der DATEV Buchhaltung (Buchungssätze zu Debitoren, insbesondere Buchungsbeträge, Rechnungsnummern, Buchungstexte, Konten, Gegenkonten, Buchungsdaten, Rechnungsdaten, Zahlungskonditionen)

Debitorenstammdaten (insbesondere Namen, Nachnamen, Firmennamen, Adressen der Debitoren, Steuernummern, USt. ID Nummern, Kontaktinformationen, wie E-Mail Adressen und Telefonnummern)

Stammdaten des Auftraggebers (insbesondere Namen, Firmennamen, Adresse, USt. ID Nummer, Herkunftsland, Zeitzone, Logo, Briefpapier)

Riecken Webservice & Application GmbH
Kaiserstr. 10
A – 1070 Wien

E office@riecken-webservices.at
T +43 1 375 00 51

(3) Von der Verarbeitung der Daten betroffen sind:

Kunden bzw. Nutzer der Debitorcloud

Kunden der Debitorcloud Nutzer

II. Dauer der Vereinbarung

(1) Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit sofortiger gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt

III. 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.

IV. Ort der Durchführung der Datenverarbeitung

(1) Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

Riecken Webservice & Application GmbH
Kaiserstr. 10
A – 1070 Wien

E office@riecken-webservices.at
T +43 1 375 00 51

V. Sub Auftragsverarbeiter

(1) Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

- OVH GmbH, Dudweiler Landstraße 5, 55123 Saabrücken, Hosting Provider für den Betrieb dedizierter Server
- Mailjet SAS, 13-13 bis Rue de l'Aubrac – 75012 Paris, Provider für das Versenden von E-Mails mit Mahnungen & Newslettern
- Österreichische Post Aktiengesellschaft, Unternehmenszentrale Rochusplatz 1, 1030 Wien, Österreich, Druck, Kuvertierung und Versand von Postbriefen innerhalb Österreichs, sowie E-Post Versand
- GoCardless Ltd. Sutton Yard, 65 Goswell Road, London, EC1V 7EN, United Kingdom, Dienstleister für Abwicklung von SEPA Lastschriften
-

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, 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 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.

VI. Geheimhaltungsverpflichtung

(1) (Sämtliche Informationen, Dokumente, Mitteilungen, Auskünfte und Daten, die der Dienstleister vom Auftraggeber sowie seinen Bevollmächtigten oder sonstigen Personen (wie zB Steuerberatern oder Rechtsanwälten) zur Erfüllung der Dienstleistung erhält, werden vom Dienstleister streng vertraulich behandelt und geheim gehalten.

Riecken Webservice & Application GmbH
Kaiserstr. 10
A – 1070 Wien

E office@riecken-webservices.at
T +43 1 375 00 51

Wien, 23.01.2017

Auftraggeber

Dienstleister, Niklas Riecken, CEO

Riecken Webservice & Application GmbH
Kaiserstr. 10
A – 1070 Wien

E office@riecken-webservices.at
T +43 1 375 00 51

Anlage ./1 – Technisch-organisatorische Maßnahmen

I. Vertraulichkeit

(1) Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu den Büroräumen, in denen ein Zugriff auf die Datenverarbeitungssysteme im Rechenzentrum besteht mit Schlüssel und Code gesichertes Türschloss. Zutritt nur durch Mitarbeiter, sowie Gesellschafter.

(2) Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch mehrere Sicherheitsebenen, Passwörter inkl. Strength Policy, Zwei Faktorenauthentifizierung, die an den Fingerabdruck gebunden ist, inkl. Security Policy, SSH Keys, für Zugriff auf Linux Maschinen, Zugriff auf Datenverarbeitende Systeme nur aus bereits vorgelagertem, gesichertem System möglich.

(3) Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten;

(4) Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

(5) Klassifikationsschema für Daten: Aufgrund Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

(6) Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, bei E-Mail via Digitale Signatur

(7) Eingabekontrolle: Protokollierung des Datenimports

(8) 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;

(9) Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

(10) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Riecken Webservice & Application GmbH
Kaiserstr. 10
A – 1070 Wien

E office@riecken-webservices.at
T +43 1 375 00 51

(11) Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;

(12) Datenschutzfreundliche Voreinstellungen;

(13) Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.