EU Datenschutz-Grundverordnung (DSGVO)

Vereinbarung über eine Auftragsverarbeitung nach Art. 28 DSGVO

zwischen der

Riecken Webservice & Application GmbH
Firmenbuch: FN412181z
ATU68522306
Nussdorfer Straße 4/1/112
1090 Wien
Österreich

- nachstehend Dienstleister genannt -

und

- nachstehend Auftraggeber genannt -

1. Gegenstand der Dienstleistung

1.1 Der Dienstleister erbringt für den Auftraggeber folgende Leistung:
Jede über den Gegenstand der Dienstleistung hinausgehende Weitergabe von Daten an Dritte sowie jede Nutzung zu anderen Zwecken als dem Gegenstand der Dienstleistung bzw. der ordnungsgemäßen Dienstleistung ist verboten und erfolgt nicht.

Bereitstellung des Cloud Gateway, einer Infrastruktur-Lösung zum Zugriff auf DATEVconnect in on Premise Netzwerken.

1.2 Von der Verarbeitung der Daten betroffen sind:

- Der Auftraggeber
- Der Mandant, für den der Auftraggeber die Daten zur Verarbeitung übermittelt
- Geschäftspartner des Mandanten, dessen Daten der Auftraggeber zur Verarbeitung übermittelt, sofern diese in den Buchungsdaten vorhanden sind

2. Dauer der Vereinbarung

2.1 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.

3. Pflichten des Dienstleisters

3.1 Der Dienstleister verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Dienstleister 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 Dienstleisters eines schriftlichen Auftrages.

3.2 Der Dienstleister 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 Dienstleister aufrecht.

3.3 Der Dienstleister 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).

3.4 Der Dienstleister 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 Dienstleister gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Dienstleister den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

3.5 Der Dienstleister 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).

3.6 Der Dienstleister wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

3.7 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 Dienstleister verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

3.8 Nach Beendigung dieser Vereinbarung löscht oder übergibt der Dienstleister nach Weisung des Auftraggebers die im Auftrag verarbeiteten produktiven personenbezogenen Daten grundsätzlich binnen 20 Kalendertagen. Technische Protokoll- und Sicherheitslogs werden rollierend nach 60 Tagen gelöscht, soweit keine längere Sicherung wegen eines Sicherheitsvorfalls, einer gesetzlichen Pflicht, eines anhängigen Verfahrens, eines konkreten Streitfalls oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Onboarding-, Vertrags-, Abrechnungs- und Berechtigungsnachweise, insbesondere Nachweise über freigegebene Softwarepartner, freigegebene DATEV-Bestände, freigegebene Programmrechte bzw. Berechtigungen, Vertragsannahme, Signatur- und Identitätsnachweise, Zeitpunkte, Vertragsversionen und Abrechnungsgrundlagen, werden für sieben Jahre ab Schluss des Kalenderjahres der letzten relevanten Leistung, Freigabe, Änderung oder Abrechnung aufbewahrt. Diese Daten werden nur zu Nachweis-, Abrechnungs-, Compliance- und Rechtsverteidigungszwecken verarbeitet und auf das hierfür erforderliche Maß beschränkt. Eine laufende Speicherung der eigentlichen DATEV-Inhaltsdaten erfolgt zu diesem Nachweiszweck nicht.

3.9 Der Dienstleister hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

3.10 Der Dienstleister verpflichtet sich, seine technisch-organisatorischen Maßnahmen mindestens einmal jährlich zu überprüfen und in angemessenem Umfang dem Stand der Technik anzupassen.

3.11 Sofern gesetzlich zulässig informiert der Dienstleister den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sich diese auf diesen Auftrag beziehen.

3.12 Der Dienstleister verpflichtet sich dazu, seine beauftragten Subunternehmer in angemessenen Zeitabständen und angemessenem Umfang darauf hin zu überprüfen, ob diese im Sinne der DSGVO als geeignete Dienstleister einzustufen sind.

3.13 **Meldung von Datenschutzverletzungen.** Der Dienstleister informiert den Auftraggeber über Verletzungen des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO sowie sonstige Sicherheitsvorfälle, die die im Auftrag verarbeiteten Daten betreffen, unverzüglich nach Bekanntwerden, spätestens jedoch binnen 48 Stunden. Der Dienstleister berücksichtigt dabei, dass der Auftraggeber als Verantwortlicher eine Verletzung nach Art. 33 Abs. 1 DSGVO binnen 72 Stunden nach Bekanntwerden der Aufsichtsbehörde zu melden hat, und gestaltet Erstmeldung und Nachlieferungen so, dass der Auftraggeber diese Frist wahren kann.

3.14 **Ansprechpartner und Eskalationswege.** Die Meldung erfolgt per E-Mail an die vom Auftraggeber bei der Registrierung angegebene E-Mail-Adresse. Der Auftraggeber stellt die Erreichbarkeit dieser Adresse sicher und teilt Änderungen dem Dienstleister an support@riecken.io mit. Ansprechpartner des Dienstleisters für Datenschutzverletzungen ist der Support des Dienstleisters unter support@riecken.io. Meldungen des Auftraggebers zu vermuteten oder festgestellten Datenschutzverletzungen an diese Adresse werden mit hoher Priorität behandelt; die Eskalation an die Geschäftsführung des Dienstleisters erfolgt über dieselbe Adresse unter Kennzeichnung als Datenschutzvorfall.

3.15 **Mindestinhalt der Erstmeldung und Statusinformationen.** Die Erstmeldung enthält, soweit dem Dienstleister zu diesem Zeitpunkt bekannt:
• Art der Verletzung sowie Zeitpunkt des Eintritts und des Bekanntwerdens;
• betroffene Systeme und Kategorien personenbezogener Daten sowie, soweit möglich, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze;
• wahrscheinliche Folgen der Verletzung;
• bereits ergriffene oder vorgeschlagene Maßnahmen zur Behebung und Eindämmung;
• Ansprechpartner beim Dienstleister für weitere Informationen.
Noch nicht verfügbare Angaben werden ohne schuldhaftes Zögern nachgereicht. Laufende Statusinformationen zu Vorfällen, die die Cloud-Gateway-Infrastruktur betreffen, veröffentlicht der Dienstleister unter https://cloudgateway-status.eu; wesentliche neue Erkenntnisse sowie der Abschluss des Vorfalls werden dem Auftraggeber zusätzlich per E-Mail mitgeteilt.

3.16 **Unterstützung bei der Vorfallbearbeitung.** Der Dienstleister unterstützt den Auftraggeber auf Anfrage an support@riecken.io bei der Bewertung des Vorfalls, seiner Eindämmung, der Dokumentation nach Art. 33 Abs. 5 DSGVO sowie bei einer etwaigen Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO und der Benachrichtigung betroffener Personen nach Art. 34 DSGVO. Er stellt dem Auftraggeber hierfür die ihm vorliegenden Informationen und Protokolle zur Verfügung, soweit sie den Vorfall betreffen.

4. Ort der Durchführung

4.1 Cloud-Gateway-Produktivdaten und das Hosting der Cloud-Gateway-Infrastruktur werden ausschließlich innerhalb der EU bzw. des EWR verarbeitet. Unterstützende Kommunikations- und Office-Dienste werden im Rahmen der jeweiligen EU-/EWR-Konfiguration eingesetzt, soweit dies vertraglich und technisch verfügbar ist.

5. Sub Auftragsverarbeiter

5.1 Der Dienstleister ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

• **OVH GmbH**, Dudweiler Landstraße 5, 55123 Saabrücken, Hosting Provider für den Betrieb dedizierter Server
• **Österreichische Post Aktiengesellschaft**, Unternehmenszentrale Rochusplatz 1, 1030 Wien, Österreich, Druck, Kuvertierung und Versand von Postbriefen innerhalb Österreichs, sowie E-Post Versand
• **GoCardless SAS**, 23 Avenue MacMahon, 75017 Paris, Frankreich Auftraggeber für Abwicklung von SEPA Lastschriften gegenüber Softwarepartnern
• **Troii Software GmbH**, Industriezeile 54, 5280 Braunau am Inn, Österreich, Zeiterfassungssoftware für Arbeits- und Projektzeiten inkl. Notizerfassung
• **Alpenländischer Kreditorenverband**, Schleifmühlgasse 2, 1941 Wien, Österreich, Dienstleister für das Einholen von Kreditauskünften, Inkasso
• **DATEV.at GmbH**, Strohgasse 14c, 1030 Wien, Österreich, Unterstützung in DATEV spezifischen Anwendungsfragen in Zusammenarbeit mit dem Kunden bzw. Kundenbeständen
• **DATEV eG**, Paumgartnerstraße 6-14, 90429 Nürnberg, Unterstützung in DATEV spezifischen Anwendungsfragen in Zusammenarbeit mit dem Kunden bzw. Kundenbeständen
• **Messagebird GmbH**, Neuer Wall 63-2 & 63-2, 20354 Hamburg, Deutschland, Anbieter für das Versenden von SMS
• **Pcvisit Software AG**, Manfred-von-Ardenne-Ring 20, 10999 Dresden, Deutschland, Fernwartungsdienstanbieter
• **Microsoft Ireland Operations Limited**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland, Anbieter von Microsoft 365 / Office 365 (insbesondere Exchange Online) im Rahmen der EU-Tenant- bzw. EU-/EWR-Datenhaltung, soweit vertraglich und technisch verfügbar; kein Hosting Provider für Cloud-Gateway-Produktivdaten

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls vorweg untersagen kann. Der Dienstleister 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 Dienstleister auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Dienstleister gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6. Geheimhaltungsverpflichtung

6.1 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 Dienst¬leistung erhält, werden vom Dienstleister streng vertraulich behandelt und geheim gehalten. Der Dienstleister verpflichtet sich insbesondere, fremde Geheimnisse im Sinne des §203 StGB (Deutschland), die ihm bei Ausübung oder bei Gelegenheit seiner Tätigkeit bekannt werden, nicht unbefugt zu offenbaren.

6.2 Der Dienstleister verpflichtet sich dazu, sich nur insoweit Kenntnis von Daten des Auftraggebers zu verschaffen, als dies zur Vertragserfüllung erforderlich ist.

6.3 Der Dienstleister erklärt, dass ihm die strafrechtlichen Folgen der Verletzung von Privatgeheimnissen gemäß §203 StGB (Deutschland), sowie dem §122 StGB (Österreich) bekannt sind.

6.4 Der Dienstleister verpflichtet alle Personen, die zur Erfüllung des Vertrags Zugriff auf Geheimnisse oder personenbezogene Daten des Auftraggebers erhalten können, insbesondere Mitarbeitende, Organe, freie Mitarbeitende und sonstige mitwirkende Personen, vor Aufnahme der Tätigkeit in Textform zur Verschwiegenheit. Die Verpflichtung umfasst auch die besondere Geheimhaltungspflicht nach §203 StGB, soweit berufsrechtliche Geheimnisse des Auftraggebers oder seiner Mandanten betroffen sind.

7. Haftung

7.1 Die Haftung für Datenschutzverletzungen richtet sich nach den gesetzlichen Bestimmungen und, soweit gesetzlich zulässig, nach den diesem Vertrag zugrunde liegenden allgemeinen Geschäftsbedingungen. Zwingende gesetzliche Ansprüche, insbesondere nach Art. 82 DSGVO, bleiben unberührt.

Anlage ./1 – Technisch-organisatorische Maßnahmen

• 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.
• 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.
• 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;
• Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
• Klassifikationsschema für Daten: Aufgrund Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).
• Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, bei E-Mail via Digitale Signatur
• Eingabekontrolle: Protokollierung des Datenimports
• 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;
• Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.
• 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, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISOZertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.

_____

Unterschrift des Auftraggebers