kanzlei-import.at

Vereinbarung

über eine Auftragsverarbeitung

gemäß Art. 28 DSGVO

Version 2.0 | Stand: 20.03.2026

DER VERANTWORTLICHE (AUFTRAGGEBER)

Firma / Name: _____

Straße, Hausnummer: _____

PLZ, Ort: _____

Firmenbuchnummer (falls vorhanden): _____

Ansprechperson: _____

E-Mail: _____

Telefon: _____

— und —

DER AUFTRAGSVERARBEITER (AUFTRAGNEHMER)

Wogenfels GmbH

Pribelsdorf 87, 9125 Eberndorf

Firmenbuchnummer: 494514b | Firmengericht: Landesgericht Klagenfurt

schließen nachfolgende Vereinbarung über die Auftragsverarbeitung (nachfolgend „AVV“) ergänzend zu den Allgemeinen Geschäftsbedingungen (AGB) bzw. dem SaaS-Nutzungsvertrag in der jeweils gültigen Fassung.

1. Gegenstand der Vereinbarung

(1) Gegenstand: Der Gegenstand des Auftrags ergibt sich aus dem Rahmenvertrag, konkret den Allgemeinen Geschäftsbedingungen (AGB) bzw. dem SaaS-Nutzungsvertrag in der jeweils gültigen Fassung, auf die hier verwiesen wird. Diese Vereinbarung ist als Ergänzung zu diesen AGB zu verstehen.

(2) Art und Zweck der Verarbeitung: Bereitstellung einer SaaS-Lösung zur Konvertierung von Buchhaltungsdateien, Rechnungen, Bankexporten und sonstigen Belegen (inkl. PDF-Dokumenten) in Import-Dateien für Buchhaltungssysteme (z.B. BMD). Der Zweck umfasst die Entgegennahme, strukturelle Umwandlung und Bereitstellung der konvertierten Daten zum Download.

Hinweis zum Einsatz von Künstlicher Intelligenz (KI): Ein KI-gestützter Assistenzdienst wird bei der initialen Einrichtung (Import-Wizard) zur Erstellung der Konvertierungslogik (Python-Skripte) sowie bei späteren Anpassungen dieser Skripte via Chat-Funktion verwendet. Um dem KI-Modell den nötigen Kontext zur effizienten Erstellung der Skripte zu geben, können hierbei durch den Auftraggeber auch produktive Echtdaten (z.B. Belegmuster, Kontonummern, Aufwandskonten) in den Wizard/Chat eingegeben und an das KI-Modell übermittelt werden. Der spätere, reguläre Produktivbetrieb (Auswahl des Konverters, Hochladen der Dateien, automatisierte Konvertierung und Download) erfolgt rein regelbasiert und ohne Datenübermittlung an KI-Modelle.

Je nach Einstellung des Auftraggebers werden die Daten entweder nach der Konvertierung umgehend gelöscht oder temporär (für maximal 90 Tage) zwischengespeichert.

(3) Art der Daten: Folgende Datenkategorien werden verarbeitet:

- Personenstammdaten (Name, Titel)
- Adress- und Kontaktdaten
- Bank-, Zahlungs- und Kontodaten
- Vertrags- und Abrechnungsdaten
- Sonstige in den hochgeladenen Dokumenten (Buchhaltungsdateien wie CSV, TXT, Excel, Lieferscheine, ERP-Exporte, Rechnungen) enthaltene personenbezogene Daten

(4) Kategorien betroffener Personen: Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- Kunden, Lieferanten und Geschäftspartner des Auftraggebers
- Mitarbeiter des Auftraggebers (z.B. bei Verarbeitung von Lohnverrechnungsdaten oder Sachbearbeiter-Kennungen auf Dateien)

2. Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages (AGB / SaaS-Nutzungsvertrag). Er endet automatisch mit Beendigung des Hauptvertrages. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Rechte und Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der beauftragten Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Auftraggeber verantwortlich. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem elektronischen Format.

Der Auftraggeber hat das Recht, dem Auftragnehmer jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder datenschutzrechtliche Unregelmäßigkeiten feststellt.

4. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge und dokumentierten Weisungen des Auftraggebers zu verarbeiten. 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.

Erhält der Auftragnehmer einen behördlichen Auftrag oder unterliegt er einer sonstigen gesetzlichen Verpflichtung, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die anfragende Stelle an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

Information bei rechtswidrigen Weisungen: Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen die DSGVO oder andere anwendbare Datenschutzbestimmungen verstößt.

Wahrung der Vertraulichkeit und Verschwiegenheit: 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.

Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich im Anhang (Technisch-organisatorische Maßnahmen).

Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte 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. 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 vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer durchzuführen.

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen sowie Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und an betroffene Personen.

Informations- und Nachweispflichten: Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle eingeräumt und der Auftragnehmer ermöglicht Überprüfungen (einschließlich Inspektionen) durch den Auftraggeber oder einen von diesem beauftragten Prüfer.

Rückgabe und Löschung nach Auftragsende: Der Auftragnehmer ist nach Abschluss der Verarbeitungsleistungen verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers entweder an diesen zurückzugeben oder datenschutzkonform zu löschen, sofern keine zwingende rechtliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

5. Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt (Physische Serverstandorte primär in Deutschland sowie im europäischen Wirtschaftsraum).

6. Sub-Auftragsverarbeiter

Der Auftragnehmer kann Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen. Der Auftraggeber stimmt der Beauftragung der nachfolgend angeführten Sub-Auftragsverarbeiter hiermit zu:

Nr.	Unternehmen	Dienstleistung	Standort
1	**Hetzner Online GmbH** Industriestr. 25, 91710 Gunzenhausen, DE	Primäres Server-Hosting (Backend, Konvertierungs-Engine), optionales KI-LLM Hosting	Deutschland (Nürnberg, Falkenstein)
2	**WebBuilds B.V. / ploi.io** Amperestraat 16J, 3861NC Nijkerk, NL	Servermanagement, Deployment und automatisierte Updates	EU (Niederlande)
3	**Amazon Web Services EMEA SARL** 38 Avenue John F. Kennedy, L-1855, Luxemburg	Bereitstellung von KI-Modellen („Amazon Bedrock“) ausschließlich zur Unterstützung bei der Erstellung der initialen Konvertierungslogik (Import-Wizard) sowie bei	EU (Primär Frankfurt/Main „eu-central-1“; bei Überlast des Standortes kann auf andere EU-Standorte ausgewichen werden)

		punktuellen Aktualisierungen des Skripts über eine Chat-Funktion. Hierbei können zur Kontextbereitstellung produktive Echtdaten (z.B. Belegmuster), die der Auftraggeber eingibt, verarbeitet werden. Im regulären Produktivbetrieb (laufende Konvertierung von Anwender-Dateien) findet keine Übermittlung von zu konvertierenden Daten an diesen Dienstleister statt.	

Besondere Zusicherungen beim Einsatz von Künstlicher Intelligenz (KI) und Cloud-Diensten:

- Kein KI-Training mit Kundendaten: Der Auftragnehmer stellt vertraglich sicher, dass die über den Sub-Auftragsverarbeiter Amazon Web Services (AWS Bedrock) verarbeiteten Echtdaten des Auftraggebers nicht für das Training, die Verbesserung oder das Fine-Tuning der zugrundeliegenden KI-Basismodelle von AWS oder Dritten verwendet werden. Die Daten dienen ausschließlich der temporären Verarbeitung zur Beantwortung der konkreten Anfrage (Skripterstellung).
- Mögliche Drittlandsübermittlung im Supportfall: Die reguläre Verarbeitung durch AWS findet innerhalb der EU statt. Sollte in absoluten Ausnahmefällen (z.B. globaler 24/7-Support durch AWS, „Follow-the-Sun“) ein rein administrativer Zugriff aus einem Drittland (z.B. USA) erfolgen, ist dies durch den Abschluss von EU-Standardvertragsklauseln (SCC) bzw. durch das EU-US Data Privacy Framework (DPF) rechtlich abgesichert.

Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel bestehender Unterauftragnehmer sind zulässig, soweit der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab in Textform anzeigt und der Auftraggeber nicht schriftlich Einspruch erhebt.

Dabei stellt der Auftragnehmer sicher, dass dem Sub-Auftragsverarbeiter vertraglich dieselben Datenschutzpflichten auferlegt werden, die in diesem Vertrag zwischen Auftraggeber und Auftragnehmer festgelegt sind (gemäß Art. 28 Abs. 4 DSGVO). Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber vollumfänglich für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Unterschriften

Durch die Unterzeichnung dieser Vereinbarung bestätigen beide Parteien, dass sie die vorstehenden Regelungen zur Auftragsverarbeitung gemäß Art. 28 DSGVO gelesen, verstanden und akzeptiert haben.

Ort, Datum	Ort, Datum
Unterschrift Auftraggeber *(Name in Blockschrift, Funktion)*	Unterschrift Auftragnehmer *(Wogenfels GmbH)*
Firmenstempel (falls vorhanden)	*Firmenstempel*

kanzlei-import.at

Anhang – Technisch-organisatorische Maßnahmen (TOMs)

1. Vertraulichkeit

- Zutrittskontrolle: Physischer Schutz der Datenverarbeitungsanlagen wird durch die strengen Richtlinien der ISO 27001 zertifizierten Rechenzentren der Hetzner Online GmbH sowie von AWS sichergestellt (elektronische Zutrittskontrollsysteme, Videoüberwachung, 24/7 Sicherheitspersonal, Hochsicherheitszäune).
- Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch zwingende Passwortrichtlinien. Zugang zu den Servern erfolgt ausschließlich netzwerkseitig abgesichert per SSH (Public-Key-Verfahren, keine reinen Passwort-Logins). Für Zugänge zu den Verwaltungsoberflächen der Infrastruktur (Hetzner, Ploi, AWS) wird Zwei-Faktor-Authentifizierung (2FA) eingesetzt.
- Zugriffskontrolle: Vergabe von Berechtigungen auf „Need-to-know"-Basis. Es besteht ein Berechtigungskonzept für Mitarbeiter.
- Trennungskontrolle: Logische Mandantentrennung in der Software-Architektur. Daten unterschiedlicher Auftraggeber werden in der SaaS-Applikation strikt getrennt verarbeitet.

2. Integrität

- Weitergabekontrolle: Sämtliche Datenübertragungen zwischen dem Client (Browser des Kunden) und den Servern sowie zwischen den Servern und den API-Endpunkten (z.B. AWS Bedrock) erfolgen zwingend verschlüsselt nach aktuellem Stand der Technik (SSL/TLS).
- Eingabekontrolle: Protokollierung von Systemereignissen (Logfiles) zur Nachvollziehbarkeit von Datenverarbeitungsprozessen.
- System-Updates: Automatisierte und zeitnahe Einspielung von Sicherheitsupdates und Patches auf Serverebene (gesteuert via ploi.io), um Sicherheitslücken präventiv zu schließen.

3. Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Die Infrastruktur wird in hochverfügbaren Rechenzentren (redundante Stromversorgung, Klimatisierung, Brandschutz) betrieben.
- Backups: Es werden regelmäßige Sicherungen über den Hetzner Backup Service durchgeführt, um Daten im Falle eines physischen oder technischen Zwischenfalls rasch wiederherstellen zu können.
- Löschkonzept (Privacy by Design): Die Software verfügt über automatisierte Löschroutinen. Konvertierungsdaten werden entsprechend den vom Auftraggeber vorgenommenen Einstellungen im System entweder unverzüglich nach dem Download oder automatisiert nach maximal 90 Tagen unwiderruflich gelöscht.

4. Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Überprüfung der Infrastruktur-Sicherheit.
- Datenschutzfreundliche Voreinstellungen der Software („Privacy by Default" – z.B. Standardeinstellung zur raschen Löschung von Quelldateien).