Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO – zwischen RDGY Software GmbH und dem Kunden

Dieser Auftragsverarbeitungsvertrag ("AVV") ergänzt den zwischen dem Kunden (im Folgenden "Verantwortlicher") und der RDGY Software GmbH (im Folgenden "Auftragsverarbeiterin") geschlossenen Nutzungsvertrag über die SaaS-Lösung "Belegmappe" (im Folgenden "Hauptvertrag"). Er gilt für alle Verarbeitungen personenbezogener Daten, die die Auftragsverarbeiterin im Auftrag des Verantwortlichen durchführt. Sofern keine gesonderte Unterzeichnung erfolgt, gilt dieser AVV mit Abschluss des Hauptvertrags als vereinbart.

1. Parteien

Auftragsverarbeiterin:
RDGY Software GmbH
Tiergartenstrasse 132, 6020 Innsbruck
UID: ATU82660639 | FN 665064k
E-Mail: hi@belegmappe.at

Verantwortlicher:
Der Kunde gemäß den Angaben im Benutzer-Account sowie dem Hauptvertrag.

2. Gegenstand, Dauer und Art der Verarbeitung

2.1 Die Auftragsverarbeiterin erbringt für den Verantwortlichen die im Hauptvertrag beschriebenen Leistungen der SaaS-Lösung "Belegmappe" (digitale Belegverwaltung, Dokumentenspeicherung, Freigaben, optional Banktransaktionsimport).

2.2 Die Verarbeitung personenbezogener Daten durch die Auftragsverarbeiterin erfolgt ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und nach dokumentierter Weisung des Verantwortlichen.

2.3 Dieser AVV gilt für die Dauer des Hauptvertrags. Nach Beendigung des Hauptvertrags werden personenbezogene Daten des Verantwortlichen nach Ablauf der in der Datenschutzerklärung und im Hauptvertrag festgelegten Fristen gelöscht oder zurückgegeben.

3. Art der personenbezogenen Daten und Kategorien betroffener Personen

3.1 Der Verantwortliche bestimmt Art und Umfang der verarbeiteten Daten. Typischerweise verarbeitet die Auftragsverarbeiterin im Auftrag folgende Datenkategorien:

• Inhaltsdaten: hochgeladene Dokumente und Belege (z. B. Rechnungen, Quittungen, Kontoauszüge), die personenbezogene Daten Dritter enthalten können (Namen, Adressen, Bankverbindungen, Steuer-IDs),
• Metadaten: Ordnerstrukturen, Zeitstempel, Bearbeitungsstatus, Freigabe-Informationen,
• Bankdaten (optional): importierte Banktransaktionsdaten im OFX-Format.

3.2 Betroffene Personen sind typischerweise Kunden, Lieferanten, Mitarbeiter oder sonstige Geschäftspartner des Verantwortlichen, deren Daten in hochgeladenen Dokumenten enthalten sind.

4. Zweck der Verarbeitung

Die Verarbeitung dient ausschließlich der Bereitstellung der SaaS-Leistungen gemäß Hauptvertrag:

Speicherung, Abruf, Strukturierung und Freigabe von Belegen und Dokumenten im Rahmen des digitalen Belegmanagements des Verantwortlichen.

5. Pflichten der Auftragsverarbeiterin

5.1 Die Auftragsverarbeiterin verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, sie ist gesetzlich zur Verarbeitung verpflichtet. In letzterem Fall teilt sie dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern rechtlich zulässig.

5.2 Die Auftragsverarbeiterin stellt sicher, dass alle mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet sind. Da der Betrieb der SaaS-Lösung "Belegmappe" derzeit ausschließlich durch den Geschäftsführer der Auftragsverarbeiterin erfolgt, ist diese Verpflichtung bereits aufgrund der gesellschaftsrechtlichen Treuepflicht und der berufsrechtlichen Verschwiegenheit umfassend gegeben. Bei künftiger Hinzuziehung weiterer Mitarbeitender werden diese vor Tätigkeitsaufnahme schriftlich zur Vertraulichkeit verpflichtet.

5.3 Die Auftragsverarbeiterin trifft alle gemäß DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOMs) – siehe Anlage 1 dieses AVV.

5.4 Die Auftragsverarbeiterin unterstützt den Verantwortlichen nach Möglichkeit bei der Erfüllung seiner Pflichten gegenüber betroffenen Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit) sowie bei der Meldung von Datenschutzverletzungen.

5.5 Die Auftragsverarbeiterin stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung dieses AVV zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, durch den Verantwortlichen oder einen von ihm beauftragten Prüfer (mit angemessener Vorankündigung und unter Wahrung berechtigter Vertraulichkeitsinteressen).

5.6 Die Auftragsverarbeiterin unterrichtet den Verantwortlichen unverzüglich, wenn eine Weisung nach ihrer Auffassung gegen DSGVO oder sonstiges anwendbares Datenschutzrecht verstößt.

6. Pflichten des Verantwortlichen

6.1 Der Verantwortliche ist allein verantwortlich für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in "Belegmappe", insbesondere für das Vorliegen einer Rechtsgrundlage nach DSGVO für die von ihm veranlasste Verarbeitung.

6.2 Der Verantwortliche stellt sicher, dass er über die erforderlichen Rechtsgrundlagen verfügt, um personenbezogene Daten Dritter in die Anwendung hochzuladen und zu verarbeiten.

6.3 Weisungen des Verantwortlichen an die Auftragsverarbeiterin erfolgen in Textform (z. B. per E-Mail).

7. Unterauftragsverarbeiter

7.1 Der Verantwortliche erteilt der Auftragsverarbeiterin eine allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern. Die aktuell eingesetzten Unterauftragsverarbeiter sind in der Unterauftragsverarbeiterliste unter https://belegmappe.at/subprocessors aufgeführt.

7.2 Die Auftragsverarbeiterin informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder den Austausch von Unterauftragsverarbeitern mit einer Vorankündigungsfrist von mindestens 14 Tagen (z. B. per E-Mail oder durch Aktualisierung der

Unterauftragsverarbeiterliste). Der Verantwortliche kann gegen solche Änderungen innerhalb von 14 Tagen ab Mitteilung Widerspruch einlegen. Im Widerspruchsfall ist die Auftragsverarbeiterin berechtigt, den Hauptvertrag zum nächstmöglichen Termin zu kündigen.

7.3 Unterauftragsverarbeitern werden dieselben Datenschutzpflichten auferlegt wie der Auftragsverarbeiterin in diesem AVV.

8. Übermittlung in Drittländer

Dokumente und Anwendungsdaten werden ausschließlich auf Servern in Frankfurt am Main, Deutschland (EU) verarbeitet und gespeichert. Soweit eingesetzte Unterauftragsverarbeiter ihren Sitz außerhalb der EU/des EWR haben (insbesondere USA: Clerk, Wasabi, Fly.io), erfolgt die Übermittlung auf Basis von Standardvertragsklauseln (SCC) und/oder dem EU-US Data Privacy Framework (DPF), soweit der jeweilige Anbieter zertifiziert ist. Details finden sich in der Unterauftragsverarbeiterliste.

9. Datensicherheit – Technische und organisatorische Maßnahmen

Die Auftragsverarbeiterin setzt angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ein. Die wesentlichen Maßnahmen sind in Anlage 1 dieses AVV beschrieben.

10. Meldung von Datenschutzverletzungen

Die Auftragsverarbeiterin meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 2 DSGVO unverzüglich nach Bekanntwerden an die im Account hinterlegte E-Mail-Adresse des Verantwortlichen – in jedem Fall so rechtzeitig, dass der Verantwortliche seine eigene gesetzliche Meldefrist von 72 Stunden gegenüber der zuständigen Datenschutzbehörde (Art. 33 Abs. 1 DSGVO) einhalten kann. Die Meldung enthält mindestens die nach Art. 33 Abs. 3 DSGVO erforderlichen Informationen, soweit zum Zeitpunkt der Meldung verfügbar; fehlende Informationen werden unverzüglich nachgereicht.

11. Löschung und Rückgabe

11.1 Dem Verantwortlichen steht jederzeit ein vollständiger Self-Service-Datenexport im GoBD-konformen ZIP-Format (CSV semikolon-separiert, Original-Dokumente, index.xml) in der Anwendung zur Verfügung. Der Export kann ohne Mitwirkung der Auftragsverarbeiterin abgerufen werden.

11.2 Nach Beendigung des Hauptvertrags – bzw. unverzüglich nach ausdrücklicher Bestätigung des Verantwortlichen im Konto-Lösch-Dialog – werden sämtliche personenbezogenen Daten des Verantwortlichen unwiderruflich gelöscht (Hard-Delete von Dokumenten im Objektspeicher, Datenbankzeilen und Authentifizierungs-Datensätzen). Voraussetzung für die Löschung ist die vorherige Bestätigung, dass ein vollständiger Datenexport gemäß 11.1 vorliegt; dies dient dem Schutz vor versehentlichem Datenverlust.

11.3 Gesetzliche Aufbewahrungspflichten (z. B. Stripe-Rechnungen gem. §132 BAO / §147 AO) bleiben unberührt; entsprechende Daten werden pseudonymisiert und nach Ablauf der Aufbewahrungsfrist gelöscht.

12. Sonstige Bestimmungen

12.1 Dieser AVV ist Bestandteil des Hauptvertrags und unterliegt österreichischem Recht.

12.2 Im Widerspruchsfall zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV vor, soweit sie die Auftragsverarbeitung betreffen.

12.3 Änderungen dieses AVV bedürfen der Textform und werden mit einer Ankündigungsfrist von mindestens 30 Tagen mitgeteilt.

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Die folgenden technischen und organisatorischen Maßnahmen (TOMs) werden gemäß Art. 32 DSGVO umgesetzt:

Vertraulichkeit

• Zugriffskontrolle: rollenbasierte Berechtigungen (Least Privilege), starke Authentifizierung über Clerk mit Multi-Faktor-Option.

• Weitergabekontrolle: verschlüsselte Übertragung aller Daten via TLS/HTTPS; keine unverschlüsselte Übertragung.

• Trennungskontrolle: logische Mandantentrennung; Daten verschiedener Verantwortlicher werden getrennt gespeichert.

• Vertraulichkeitsverpflichtung aller mit der Verarbeitung befassten Mitarbeiter.

Integrität

• Eingabekontrolle: Protokollierung sicherheitsrelevanter Ereignisse und Zugriffe.

• Übertragungsintegrität: TLS mit aktuellen Cipher-Suites.

• Manipulationssicheres Audit-Log mit SHA-256-Hash-Chain für Beleg-Statusübergänge.

Verfügbarkeit und Belastbarkeit

• Speicherung auf redundanter S3-Infrastruktur (Wasabi, Frankfurt/EU) mit serverseitiger AES-256-Verschlüsselung und Object-Versionierung.

• Datenbank-Backups durch Fly.io Managed Postgres (automatische tägliche Snapshots, Point-in-Time-Recovery für mindestens 7 Tage).

• Zusätzlicher Self-Service-Export im GoBD-Format jederzeit abrufbar; Verantwortliche können dadurch eigenständig kundenseitige Sicherungskopien erstellen.

• Hosting auf Fly.io mit automatischem Neustart bei Ausfällen (Frankfurt/EU-Region).

Verfahren zur regelmäßigen Überprüfung

• Regelmäßige Überprüfung und Aktualisierung der TOMs.

• Schwachstellenmanagement: zeitnahe Einspielung von Sicherheitsupdates für alle Systemkomponenten.

• Datenschutz durch Technikgestaltung (Privacy by Design) bei der Entwicklung neuer Funktionen.

Stand: 26. Mai 2026

Unterschriften

Ort, Datum: _____

Auftragsverarbeiterin (RDGY Software GmbH):

_____

Unterschrift / Stempel

Verantwortlicher (Kunde):

_____

Unterschrift / Stempel