

Auftragsverarbeitungsvereinbarung (AVV)

gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO) zwischen dem nachfolgend genannten Auftraggeber (Verantwortlicher) und MintFolder AI UG (haftungsbeschränkt) i.G. (Auftragsverarbeiter)

Hinweis zur Vertragsverwendung. Diese Vorlage enthält die wesentlichen Pflichtinhalte nach Art. 28 Abs. 3 DSGVO und orientiert sich an den Mustervorlagen der deutschen Datenschutz-Aufsichtsbehörden (DSK). Bitte vor Unterzeichnung den vollständigen Vertragstext durch den eigenen Datenschutzbeauftragten oder einen Rechtsanwalt prüfen lassen. Die unterschriebene PDF-Version mit ergänzten Auftraggeber-Angaben ist die rechtsverbindliche Fassung; diese Webseite dient ausschließlich der Information.

1. Vertragsparteien

AUFTRAGGEBER (VERANTWORTLICHER)

Anschrift: -----
USt-IdNr.: -----
Vertretungsberechtigt: -----
Datenschutzbeauftragte/r: -----

AUFTRAGSVERARBEITER

MintFolder AI UG (haftungsbeschränkt) i.G.

Anschrift: Sudetenstr. 18, 35039 Marburg
Registergericht: Amtsgericht Marburg, HRB [bitte nachtragen]
Geschäftsführer: Thaeer Sukay
Datenschutzkontakt: datenschutz@mintfolder.ai

2. Gegenstand und Dauer der Verarbeitung

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung der MintFolder-AI-Dienste (Belegarchivierung, KI-Klassifizierung, Datenexport). Der Auftrag wird auf der Grundlage des zugrundeliegenden Hauptvertrags (Allgemeine Geschäftsbedingungen sowie individuelle Bestellung) erbracht.

Die Vereinbarung beginnt mit Abschluss des Hauptvertrags und endet mit dessen Beendigung. Die Pflichten zur Geheimhaltung sowie die Rechtsfolgen aus Ziffer 11 (Datenrückgabe und -löschung) bleiben über das Vertragsende hinaus bestehen.

3. Art und Zweck der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zu folgenden Zwecken:

- Speicherung und revisionssichere Archivierung von Geschäftsbelegen gemäß GoBD-Grundsätzen (BMF-Schreiben vom 28. November 2019)
- Automatische Klassifizierung von Belegen über eine mehrstufige KI-Pipeline
- Erstellung von DATEV-EXTF-Buchungstapeln, XRechnungen (3.0) und ZUGFeRD-Rechnungen (2.x, PDF/A-3)
- Bereitstellung der Daten zur Volltextsuche und für das Reporting
- Backup und Wiederherstellung gemäß den unter Ziffer 7 beschriebenen Maßnahmen

Der Auftragsverarbeiter verwendet die Daten nicht für eigene Zwecke und ist insbesondere nicht berechtigt, sie zu eigenem Marketing oder zur Modellverbesserung der KI-Komponenten zu nutzen.

4. Datenkategorien und Kategorien betroffener Personen

Datenkategorien

- Stammdaten von Geschäftspartnern des Auftraggebers (Name, Anschrift, USt-IdNr., Bankverbindung)
- Belegdaten (Rechnungen, Quittungen, Verträge, sonstige Geschäftskorrespondenz)
- Buchungsdaten (Beträge, Daten, Konten gemäß SKR03 oder SKR04)
- Nutzerdaten der Mitarbeitenden des Auftraggebers (E-Mail-Adresse, Name, Rolle, Anmeldezeitpunkte, Audit-Log-Einträge)
- Soweit in Belegen enthalten: weitere personenbezogene Daten Dritter

Kategorien betroffener Personen

- Geschäftspartner und Kunden des Auftraggebers
- Mitarbeitende des Auftraggebers, die das System nutzen
- Sonstige in Belegen genannte natürliche Personen

Besondere Kategorien personenbezogener Daten [Art. 9 DSGVO](#) sind nicht Gegenstand der Verarbeitung, soweit der Auftraggeber sie nicht aktiv selbst hochlädt.

5. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter wird:

1. personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers verarbeiten Art. 28 Abs. 3 lit. a DSGVO ;
2. die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichten oder sich vergewissern, dass diese einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen lit. b ;
3. alle erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO ergreifen (siehe Ziffer 7);
4. die Bedingungen für die Inanspruchnahme von Unterauftragsverarbeitern nach Ziffer 6 einhalten;
5. den Auftraggeber bei der Erfüllung seiner Pflichten nach Art. 32 bis 36 DSGVO unterstützen;
6. nach Beendigung der Verarbeitung die personenbezogenen Daten gemäß Ziffer 11 zurückgeben oder löschen;
7. alle erforderlichen Informationen zur Verfügung stellen, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen.

6. Unterauftragsverarbeiter

Der Auftraggeber erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Hinzuziehung der nachstehend benannten Unterauftragsverarbeiter. Eine Änderung dieser Liste wird dem Auftraggeber schriftlich oder per E-Mail mit einer Frist von 30 Tagen vor Inkrafttreten mitgeteilt; der Auftraggeber kann der Änderung innerhalb dieser Frist widersprechen.

ANBIETER	SITZ / DATENVERARBEITUNGSSORT	ZWECK
IONOS SE	Deutschland (Frankfurt am Main)	Hosting der Hauptanwendung (VPS)
Cloudflare Germany GmbH	Deutschland / EU (Edge-Knoten)	Content Delivery Network, TLS-Terminierung, DDoS-Schutz
Hetzner Online GmbH	Deutschland (Falkenstein)	Verschlüsselte Backups (Restic, AES-256 client-side)
Hetzner Online GmbH (Object Storage)	Deutschland (Falkenstein)	Primärer Live-Speicher für B2B-Dokumente (Vault) via S3-kompatibles Object Storage; serverseitige Verschlüsselung at rest (AES-256) durch Hetzner. Anwendungsseitige Verschlüsselung der Dateiinhalte als zusätzliche Härtung gem. Art. 32 Abs. 1 lit. a DSGVO in Engineering-Roadmap.
Google Ireland Limited	EU (Google Drive Speicherregion)	Sekundäre verschlüsselte Backups (rclone, AES-256-CBC)
Zoho Corporation B.V.	EU (Zoho EU-Rechenzentrum, Niederlande)	Geschäftliche E-Mail-Kommunikation

ANBIETER	SITZ / DATENVERARBEITUNGSORT	ZWECK
Sendinblue GmbH (Brevo)	EU (Frankreich)	Transaktionale E-Mails (Versand)
Stripe Payments Europe Limited	EU (Irland)	Zahlungsabwicklung B2C und B2B
Google LLC (Gemini API)	EU-Region (sofern verfügbar) / USA — EU-U.S. DPF (Beschluss 2023/1795) primär; SCCs (Beschluss 2021/914) ergänzend	KI-Klassifizierung von Belegtext
Anthropic PBC (Claude API)	USA — EU-U.S. DPF (Beschluss 2023/1795) primär; SCCs (Beschluss 2021/914) ergänzend	KI-Klassifizierung von Belegtext (Fallback)
OpenAI Ireland Limited (EU-Vertragspartner) / OpenAI, LLC (verarbeitende Stelle, USA — Unterauftragsverarbeiter)	EU (Dublin, IE) als Vertragsort; Verarbeitung in den USA	KI-Klassifizierung von Belegtext (Fallback) — GPT-4o API mit Zero Data Retention ('store=False'); Übermittlung auf Grundlage von Art. 46 Abs. 2 lit. c DSGVO (SCCs) sowie — soweit der Empfänger zertifiziert ist — EU-U.S. Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795). DPF-Zertifizierungsstatus zu verifizieren vor nächstem AVV-Abschluss — Stand 2026-05-13.
Microsoft Ireland Operations Ltd / Microsoft Corporation	EU (Irland) — Microsoft EU Data Boundary; eingeschränkte Control-Plane-Operationen (Token-Rrefresh) USA	OneDrive-Integration via Microsoft Graph (Files.ReadWrite-Scope) — Aktivierung ausschließlich durch ausdrückliche Nutzeraktion (OAuth-Verbindung). Verarbeitet OAuth-Refresh-Tokens

ANBIETER	SITZ / DATENVERARBEITUNGSORT	ZWECK
		(verschlüsselt gespeichert), Datei-Metadaten und Datei- Inhalte bei expliziter Synchronisation

Übermittlungen an Unterauftragsverarbeiter mit Sitz außerhalb des EWR erfolgen ausschließlich auf Grundlage geeigneter Garantien [Art. 46 DSGVO](#), insbesondere — soweit die Empfänger nach dem EU-U.S. Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795 vom 10. Juli 2023) zertifiziert sind — auf Basis des Angemessenheitsbeschlusses für die USA als primärer Transfergrundlage; ergänzend gelten die Standardvertragsklauseln der EU-Kommission (Durchführungsbeschluss (EU) 2021/914) als zusätzliche Sicherheitsmaßnahme nach Art. 46 Abs. 2 lit. c DSGVO. Der DPF-Zertifizierungsstatus der jeweiligen Empfänger wird vor jedem AVV-Abschluss bei dataprivacyframework.gov/list verifiziert.

Die aktuellste Fassung der Liste der Unterauftragsverarbeiter ist jederzeit unter mintfolder.ai/avv abrufbar.

7. Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter ergreift die in der Anlage "[Technisch-organisatorische Maßnahmen](#)" beschriebenen Maßnahmen nach Art. 32 DSGVO. Diese Anlage ist Bestandteil dieser Vereinbarung und wird bei Bedarf aktualisiert. Der Auftraggeber wird über wesentliche Änderungen mit angemessenem Vorlauf informiert.

8. Datenschutzverletzungen

Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, informiert er den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntnisnahme. Die Mitteilung enthält mindestens:

- eine Beschreibung der Art der Verletzung mit Angabe von Kategorien und Zahl der betroffenen Personen sowie Kategorien und Zahl der betroffenen Datensätze, soweit bekannt;
- den Namen und die Kontaktdaten des Datenschutzkontakts;
- eine Beschreibung der wahrscheinlichen Folgen;
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Schadensbegrenzung.

Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung seiner Meldepflichten nach Art. 33, 34 DSGVO.

9. Unterstützung des Auftraggebers

Der Auftragsverarbeiter unterstützt den Auftraggeber im erforderlichen Umfang bei:

- der Beantwortung von Anfragen betroffener Personen [Art. 12 bis 23 DSGVO](#) ;
- der Sicherheit der Verarbeitung [Art. 32](#) ;
- der Meldung und Benachrichtigung von Verletzungen [Art. 33, 34](#) ;
- der Datenschutz-Folgenabschätzung [Art. 35](#) und der vorherigen Konsultation [Art. 36](#) .

10. Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung der Pflichten aus dieser Vereinbarung zu überprüfen. Auf Anfrage stellt der Auftragsverarbeiter die zur Beurteilung erforderlichen Informationen, insbesondere die jeweils aktuellen TOMs, zur Verfügung.

Inspektionen vor Ort werden mit angemessenem Vorlauf (mindestens 14 Tage) angekündigt und in einer Weise durchgeführt, die den ordnungsgemäßen Geschäftsbetrieb nicht beeinträchtigt. Sofern erforderlich, kann der Auftragsverarbeiter unabhängige Auditor-Berichte (z. B. nach ISO 27001 oder vergleichbaren Standards) zur Erfüllung der Kontrollanforderungen vorlegen.

11. Vertragsbeendigung und Datenrückgabe

Nach Beendigung dieser Vereinbarung wird der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers entweder:

- in einem strukturierten, gängigen und maschinenlesbaren Format an den Auftraggeber zurückgeben (DATEV-EXTF, JSON, CSV), oder
- vollständig löschen, einschließlich vorhandener Sicherungskopien.

Die Löschung erfolgt innerhalb von 30 Tagen nach Vertragsende; Sicherungskopien werden nach Ablauf der jeweiligen Aufbewahrungszyklen (maximal 90 Tage) ebenfalls gelöscht. Die Löschung wird auf Wunsch schriftlich bestätigt.

Soweit gesetzliche Aufbewahrungspflichten [§ 147 AO](#), [§ 257 HGB](#) einer sofortigen Löschung entgegenstehen, werden die betroffenen Daten lediglich gesperrt (Zugriff ausgeschlossen, Speicherung fortgesetzt) und nach Ablauf der Frist gelöscht.

12. Schlussbestimmungen

Vorrangregelung. Im Falle von Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag haben die Regelungen dieser Vereinbarung in datenschutzrechtlichen Belangen Vorrang.

Änderungen. Änderungen und Ergänzungen bedürfen der Schriftform (Textform per E-Mail genügt). Dies gilt auch für die Änderung dieser Schriftformklausel.

Salvatorische Klausel. Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien werden eine unwirksame Bestimmung durch eine wirksame ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Bestimmung möglichst nahekommt.

Anwendbares Recht und Gerichtsstand. Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters (Marburg).

Unterschriften

AUFTRAGGEBER

Ort, Datum:

Unterschrift:

Name in Druckbuchstaben:

AUFTRAGSVERARBEITER

Ort, Datum:

Unterschrift:

Name in Druckbuchstaben: Thaeer Sukay (Geschäftsführer)

MintFolder AI UG (haftungsbeschränkt) i.G. · Sudetenstr. 18, 35039 Marburg · Impressum · Datenschutz ·
TOMs

Stand dieser Fassung: 2026-05-10. Letzte Aktualisierung der Unterauftragsverarbeiter-Liste: 2026-05-10.

Bei Druck: Bitte mit Datum und Unterschrift versehen und an datenschutz@mintfolder.ai senden.