Auftragsverarbeitungsvertrag (AVV)

Version 1.1 · Stand 06.10.2026

Präambel und Vertragsschluss

Die Mehr.Wert Gruppe GmbH, Anny Wödl Gasse 3, 2700 Wiener Neustadt, Österreich (nachfolgend „Auftragsverarbeiter") stellt mit dem Belegmanager eine Software zur Buchhaltungsvorbereitung bereit. Der Nutzer dieser Software (nachfolgend „Verantwortlicher") bleibt für die von ihm eingebrachten personenbezogenen Daten datenschutzrechtlich verantwortlich.

Dieser Vertrag konkretisiert die Pflichten beider Seiten nach Art. 28 DSGVO. Er ist **Bestandteil der Allgemeinen Geschäftsbedingungen und des Nutzungsvertrags und bedarf keiner gesonderten Unterzeichnung.** Mit der Zustimmung zu den Allgemeinen Geschäftsbedingungen gilt er als geschlossen. Eine gegengezeichnete Fassung stellt der Auftragsverarbeiter auf Wunsch zur Verfügung.

Dieser Vertrag gilt ausschließlich für Verarbeitungen, die der Auftragsverarbeiter im Auftrag des Verantwortlichen durchführt. Verarbeitungen personenbezogener Daten für eigene Zwecke des Auftragsverarbeiters – insbesondere Vertragsverwaltung, Abrechnung, Zahlungsabwicklung, allgemeine kaufmännische Kundenbetreuung ohne Verarbeitung der vom Verantwortlichen eingebrachten Daten, Erfüllung eigener gesetzlicher Pflichten sowie Geltendmachung oder Abwehr von Rechtsansprüchen – erfolgen in eigener Verantwortlichkeit und richten sich nach seiner Datenschutzerklärung. Soweit im Rahmen des technischen oder fachlichen Supports auf im Auftrag verarbeitete Beleg-, Zahlungs- oder sonstige Daten des Verantwortlichen zugegriffen wird, erfolgt diese Verarbeitung als Auftragsverarbeitung nach diesem Vertrag.

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der vertraglich vereinbarten Softwareleistung. Einzelheiten regelt **Anlage 1**.

(2) Die Laufzeit entspricht der des Nutzungsvertrags. Die Pflichten zur Löschung und Rückgabe nach § 11 bestehen darüber hinaus fort.

§ 2 Begriffsbestimmungen

Die Begriffe dieses Vertrags entsprechen den Definitionen des Art. 4 DSGVO.

§ 3 Gegenstand, Art und Zweck der Verarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vereinbarten Softwareleistung: Erfassung, Auslesung, Ordnung und Zuordnung von Belegen, Abgleich mit Zahlungsvorgängen sowie Bereitstellung von Auswertungen und Übergabepaketen.

(2) Art der Verarbeitung, Kategorien betroffener Personen und Kategorien personenbezogener Daten ergeben sich aus **Anlage 1**.

(3) Die Software ist nicht auf die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO ausgerichtet. Aufgrund der Art von Rechnungs- und Belegdaten – etwa Rechnungen von Ärzten, Apotheken oder Therapeuten – lässt sich deren Verarbeitung im Einzelfall jedoch nicht ausschließen. Der Verantwortliche bringt solche Daten nur ein, soweit hierfür eine Rechtsgrundlage nach Art. 6 und gegebenenfalls Art. 9 DSGVO besteht. Der Auftragsverarbeiter verarbeitet diese Daten wie alle übrigen Belegdaten ausschließlich auf Weisung und wertet sie nicht gesondert aus.

§ 4 Pflichten des Auftragsverarbeiters

(1) **Weisungsbindung.** Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, auch hinsichtlich einer Übermittlung in ein Drittland oder an eine internationale Organisation. Die Erbringung der vertraglich vereinbarten Leistung nach § 3 gilt als dokumentierte Weisung. Eine Verarbeitung der im Auftrag verarbeiteten Daten zu eigenen Zwecken findet nicht statt. Dies gilt nicht, soweit der Auftragsverarbeiter durch das Recht der Europäischen Union oder eines Mitgliedstaats zu einer Verarbeitung verpflichtet ist; in diesem Fall teilt er dem Verantwortlichen diese rechtliche Verpflichtung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) **Vertraulichkeit.** Zur Verarbeitung eingesetzte Personen sind zur Vertraulichkeit verpflichtet. Zugriff besteht nach dem Grundsatz der Erforderlichkeit.

(3) **Sicherheit der Verarbeitung.** Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (§ 6, **Anlage 2**).

(4) **Unterstützung.** Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Beantwortung von Betroffenenanfragen (Art. 15 bis 22 DSGVO) sowie bei dessen Pflichten nach Art. 32 bis 36 DSGVO. Anfragen richtet der Verantwortliche in Textform an office@online-mehrwert.at; der Auftragsverarbeiter stellt die benötigten Auskünfte, Auszüge oder Löschungen unverzüglich, in der Regel innerhalb von fünf Werktagen, bereit, soweit sie der Verantwortliche nicht selbst über die Software vornehmen kann. Anfragen betroffener Personen, die beim Auftragsverarbeiter eingehen, leitet dieser unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst.

(5) **Hinweispflicht.** Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen Datenschutzrecht verstößt, teilt er dies unverzüglich mit. Er darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen.

(6) **Nachweise.** Der Auftragsverarbeiter stellt dem Verantwortlichen die zum Nachweis der Einhaltung dieses Vertrags erforderlichen Informationen zur Verfügung (§ 10).

§ 5 Weisungsrecht des Verantwortlichen

(1) Weisungen erfolgen in Textform. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(2) Der Verantwortliche kann die Weisungen jederzeit konkretisieren. Führt eine Weisung zu Mehraufwand, der über die vertraglich geschuldete Leistung hinausgeht, kann der Auftragsverarbeiter hierfür eine angemessene Vergütung verlangen; er weist vorher darauf hin.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter setzt die in **Anlage 2** beschriebenen Maßnahmen um und dokumentiert sie.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie anpassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

§ 7 Unterauftragsverarbeiter

(1) **Allgemeine Genehmigung.** Der Verantwortliche erteilt die allgemeine Genehmigung zur Beauftragung weiterer Auftragsverarbeiter. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt und damit genehmigt.

(2) **Vorankündigung und Widerspruch.** Beabsichtigt der Auftragsverarbeiter, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden auszutauschen, teilt er dies dem Verantwortlichen **mindestens 14 Tage vorher** in Textform mit. Der Verantwortliche kann der Änderung **innerhalb von 14 Tagen ab Zugang der Mitteilung** aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Widerspricht er nicht, gilt die Genehmigung als erteilt. Erhebt der Verantwortliche fristgerecht Widerspruch, wird die beabsichtigte Änderung ihm gegenüber bis zur Klärung des Widerspruchs nicht umgesetzt.

(3) **Folge eines Widerspruchs.** Betrifft der Widerspruch einen Unterauftragsverarbeiter, der ausschließlich für eine optionale Funktion eingesetzt wird (etwa WhatsApp-Belegeingang, Postfachanbindung oder Portalabruf), wird diese Funktion für den Verantwortlichen deaktiviert; die übrige Leistung bleibt unberührt. Kann der Auftragsverarbeiter die Leistung ohne den betroffenen Unterauftragsverarbeiter nicht in gleicher Weise erbringen, sind beide Seiten berechtigt, den Nutzungsvertrag zum Zeitpunkt der geplanten Änderung zu kündigen. Bereits im Voraus gezahlte Entgelte werden anteilig erstattet.

(4) **Vertragliche Bindung.** Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter auf Datenschutzpflichten, die den Pflichten dieses Vertrags entsprechen. Er bleibt dem Verantwortlichen gegenüber für deren Einhaltung verantwortlich.

(5) **Drittlandtransfer.** Findet eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums statt, stellt der Auftragsverarbeiter geeignete Garantien nach Kapitel V DSGVO sicher – durch EU-Standardvertragsklauseln, den EU-US-Datenschutzrahmen oder einen Angemessenheitsbeschluss. Der jeweils tragende Mechanismus ist in **Anlage 3** je Unterauftragsverarbeiter ausgewiesen.

(6) Nicht als Unterauftragsverarbeitung im Sinne dieses Paragraphen gelten Nebenleistungen ohne Bezug zu den verarbeiteten Daten, etwa Telekommunikations- oder Reinigungsdienste.

§ 8 Datenschutz-Folgenabschätzung

Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer vorherigen Konsultation nach Art. 36 DSGVO, insbesondere durch Bereitstellung der erforderlichen Informationen über die Verarbeitung.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich nach Kenntniserlangung; eine erste Meldung erfolgt **grundsätzlich innerhalb von 24 Stunden**. Noch nicht verfügbare Angaben werden ohne unangemessene Verzögerung nachgereicht.

(2) Die Meldung enthält, soweit verfügbar: Art der Verletzung, betroffene Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, eine Anlaufstelle für Rückfragen, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen. Sind nicht alle Angaben sofort verfügbar, erfolgt die Meldung stufenweise.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Meldepflichten nach Art. 33 und 34 DSGVO.

(4) Meldungen an die Aufsichtsbehörde und an betroffene Personen obliegen dem Verantwortlichen. Der Auftragsverarbeiter nimmt sie nicht ohne dessen Weisung vor.

§ 10 Kontrollrechte des Verantwortlichen

(1) **Nachweise.** Der Auftragsverarbeiter weist die Einhaltung der Pflichten aus diesem Vertrag auf Anfrage in geeigneter Weise nach, insbesondere durch die Verfahrensdokumentation, die Beschreibung der technischen und organisatorischen Maßnahmen sowie durch Zertifizierungen und Prüfberichte der eingesetzten Unterauftragsverarbeiter.

(2) **Überprüfungen vor Ort.** Genügen diese Nachweise im Einzelfall nicht, kann der Verantwortliche eine Überprüfung durchführen oder durch einen Prüfer durchführen lassen, der fachlich geeignet und zur Verschwiegenheit verpflichtet ist. Der Auftragsverarbeiter kann einen vorgeschlagenen Prüfer aus nachweisbaren Gründen eines Interessenkonflikts oder zum Schutz von Geschäftsgeheimnissen ablehnen; die Parteien bestimmen dann unverzüglich einen gleichwertigen unabhängigen Prüfer. Überprüfungen sind **mindestens vier Wochen vorher** anzukündigen und während der üblichen Geschäftszeiten durchzuführen; Routineprüfungen finden **höchstens einmal je Kalenderjahr** statt. Sie dürfen den Betriebsablauf nicht unangemessen beeinträchtigen.

(3) **Ausnahmen.** Bei begründetem Verdacht einer wesentlichen Verletzung des Schutzes personenbezogener Daten, bei wesentlichen Änderungen der Verarbeitung oder auf Anordnung einer Aufsichtsbehörde entfallen die Beschränkungen nach Absatz 2 hinsichtlich Frist und Häufigkeit.

(4) **Kosten.** Die Kosten einer Überprüfung nach Absatz 2 trägt der Verantwortliche, es sei denn, dabei wird eine Pflichtverletzung des Auftragsverarbeiters festgestellt.

§ 11 Löschung und Rückgabe

(1) **Nach Vertragsende.** Nach Beendigung des Nutzungsvertrags entscheidet der Verantwortliche, ob die im Auftrag verarbeiteten Daten gelöscht oder in einem gängigen, strukturierten Format herausgegeben werden; er kann diese Entscheidung bis zum Ablauf der Frist nach Satz 2 ändern. Sofern keine abweichende Weisung erfolgt, werden die Daten nach Ablauf des bezahlten Zeitraums für einen nachvertraglichen Exportzeitraum von **60 Tagen** ausschließlich zur Bereitstellung eines Exports vorgehalten und anschließend automatisch gelöscht. Diese Frist entspricht Ziffer 6 der Allgemeinen Geschäftsbedingungen. Nach vollständiger Herausgabe löscht der Auftragsverarbeiter die im Auftrag verarbeiteten personenbezogenen Daten und vorhandene Kopien, soweit nicht eine gesetzliche Verpflichtung zur weiteren Speicherung besteht.

(2) **Während der Laufzeit.** Vom Verantwortlichen gelöschte Belege werden unverzüglich aus allen Ansichten, Auswertungen und Exporten entfernt und nicht weiter verarbeitet. Sie bleiben gespeichert, bis der Verantwortliche ihre endgültige Löschung verlangt – die dann unverzüglich erfolgt –, spätestens bis zur Löschung nach Absatz 1.

(3) **Fortbestehen in Sicherungen.** Datenbanksicherungen werden **sieben Tage** vorgehalten. Bereits gelöschte Daten können bis zum Ablauf dieser Frist in Sicherungen fortbestehen; sie werden dort nicht weiterverarbeitet und mit dem Sicherungsstand gelöscht.

(4) **Gesetzliche Aufbewahrungspflichten.** Bestehen für den Auftragsverarbeiter gesetzliche Aufbewahrungspflichten, bleibt die Löschung insoweit ausgesetzt; die Verarbeitung beschränkt sich dann auf die Erfüllung dieser Pflicht.

(5) **Aufbewahrungspflicht des Verantwortlichen.** Die Aufbewahrungspflicht nach § 132 BAO – sieben Jahre – trifft ausschließlich den Verantwortlichen und geht durch die Nutzung der Software nicht auf den Auftragsverarbeiter über. Der Belegmanager ist kein gesetzliches Archivsystem. Der Verantwortliche ist gehalten, die monatlichen Übergabepakete laufend, spätestens vor Ablauf der Frist nach Absatz 1, in eine eigene Archivierung zu übernehmen.

(6) **Bestätigung.** Der Auftragsverarbeiter bestätigt die Löschung auf Anfrage in Textform.

§ 12 Haftung

Die Haftung richtet sich nach den gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO, und im Übrigen nach den Regelungen des Nutzungsvertrags, soweit diesen nicht zwingendes Recht entgegensteht.

§ 13 Schlussbestimmungen

(1) Dieser Vertrag ist Bestandteil des Nutzungsvertrags. Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag in Fragen des Datenschutzes gehen die Regelungen dieses Vertrags vor.

(2) Änderungen bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.

(3) Ist eine Bestimmung unwirksam, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(4) Es gilt österreichisches Recht unter Ausschluss des UN-Kaufrechts. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.

Anlage 1 – Gegenstand, Art und Zweck der Verarbeitung

Gegenstand

Bereitstellung des Belegmanagers als Software zur Buchhaltungsvorbereitung: Erfassung von Belegen über verschiedene Eingangswege, maschinelle Auslesung der Belegdaten, Zuordnung zu Zahlungsvorgängen, Monatsabschluss und Erzeugung von Übergabepaketen für die Steuerberatung.

Art der Verarbeitung

Vorgang	Beschreibung
Erfassung	Belegeingang über Upload, E-Mail, angebundenes Postfach, WhatsApp und Lieferantenportale
Maschinelle Auslesung	KI-gestützte Erkennung von Belegdaten zur Vorbefüllung der Felder
Speicherung	Ablage der Belege und der erfassten Daten je Mandant
Abgleich	Zuordnung von Zahlungsvorgängen zu Belegen
Bereitstellung	Auswertungen, Übergabepakete, Export, Versand an die Steuerberatung
Nutzerverwaltung	Anmeldung, Rollen und Berechtigungen innerhalb eines Mandanten
Benachrichtigung	Versand transaktionaler E-Mails
Support	Bearbeitung von Supportanfragen; Antwortentwürfe werden KI-gestützt vorbereitet und vor dem Versand von einem Menschen geprüft

Kategorien betroffener Personen

- Nutzerinnen und Nutzer des Verantwortlichen (Inhaber, Mitarbeiter, Buchhaltung)
- Natürliche Personen auf Seiten der Geschäftspartner des Verantwortlichen (Lieferanten, Kunden, deren Ansprechpartner), soweit sie auf Belegen genannt sind
- Kontoinhaber und Zahlungsbeteiligte, soweit aus Zahlungsvorgängen ersichtlich

Kategorien personenbezogener Daten

- **Konto- und Stammdaten:** Name, E-Mail-Adresse, Telefon- und Mobilnummer, Rolle; Firmendaten des Verantwortlichen einschließlich Anschrift und UID-Nummer
- **Belege und deren Inhalte:** Rechnungsdokumente als PDF oder Bild sowie die daraus ausgelesenen Daten – Geschäftspartner, Rechnungsdatum, Rechnungsnummer, Beträge, Steuerbeträge, UID, IBAN, Zahlungsreferenzen
- **Zahlungsvorgänge:** Kontoumsätze aus Datei-Import und aus dem Abruf über die Zahlungsdiensteschnittstelle – IBAN, Buchungstext, Verwendungszweck, Betrag, Datum
- **Kassabuch:** Bareinnahmen und -ausgaben mit Beleg- und Belegkreisnummern
- **Zugangsdaten Dritter:** vom Verantwortlichen hinterlegte Zugangsdaten zu eigenen E-Mail-Postfächern und Lieferantenportalen; verschlüsselt gespeichert
- **Kommunikationsinhalte:** Absenderadresse, Betreff und Anhänge eingehender Belegmails; Absendernummer und Nachrichtentext eingehender WhatsApp-Nachrichten
- **Anmerkungen und Kommentare** zu Belegen und Zahlungsvorgängen

- **Supportvorgänge:** Tickets samt Anhängen, Verläufe des Hilfe-Assistenten sowie die zur Beantwortung herangezogenen Beleg- und Zahlungsdaten
- **Nutzungs- und Protokolldaten:** IP-Adresse, Zeitstempel sicherheitsrelevanter Vorgänge, Import- und Exportprotokolle

Besondere Kategorien nach Art. 9 DSGVO

Werden nicht gezielt verarbeitet. Siehe § 3 Abs. 3.

Anlage 2 – Technische und organisatorische Maßnahmen

Stand: 06.10.2026

Der Auftragsverarbeiter betreibt **keine eigene Serverinfrastruktur**. Die Verarbeitung findet ausschließlich bei den in Anlage 3 genannten Anbietern statt. Datenbank und Dateispeicher liegen in Rechenzentren in Frankfurt am Main, dort wird auch die Anwendung serverseitig ausgeführt; die maschinelle Auslesung erfolgt in Rechenzentren innerhalb der Europäischen Union (Abschnitt 5). Für einzelne Kommunikations-, Infrastruktur- und Integrationsdienste können Verarbeitungen in Drittländern stattfinden; diese sind in Anlage 3 ausgewiesen und nach Kapitel V DSGVO abgesichert. Es besteht **kein Publikumsverkehr** und es werden **keine personenbezogenen Daten in Papierform oder auf Wechseldatenträgern** verarbeitet. Alle Tätigkeiten erfolgen im Homeoffice.

1. Vertraulichkeit

Zutrittskontrolle

Maßnahme	Umsetzung
Eigene Rechenzentren	Keine. Die Kernsysteme für Datenbank und Dateispeicherung werden in zertifizierten Rechenzentren innerhalb der Europäischen Union betrieben. Für einzelne Kommunikations-, Infrastruktur- und Integrationsdienste werden die in Anlage 3 genannten Anbieter eingesetzt; dabei können Verarbeitungen in Drittländern stattfinden, die nach Kapitel V DSGVO abgesichert sind.
Arbeitsplätze	Homeoffice in abschließbaren privaten Räumlichkeiten; kein Publikumsverkehr, kein Zutritt Dritter zu Arbeitsgeräten.

Zugangskontrolle (Systeme)

Maßnahme	Umsetzung
Mehr-Faktor-Authentifizierung	Für sämtliche über das Internet erreichbaren Verwaltungszugänge aktiviert.
Passwortrichtlinie	Verbindlich; mindestens zwölf Zeichen mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, soweit vom jeweiligen System unterstützt.
Passwortverwaltung	Ausschließlich über einen Passwort-Manager; keine Mehrfachverwendung, keine Ablage im Klartext.
Geräteverschlüsselung	Datenträger aller eingesetzten mobilen Geräte sind vollständig verschlüsselt.

Bildschirmsperre	Automatische Sperre nach definierter Zeit der Inaktivität.
Schadsoftwareschutz	Aktueller Virenschutz auf allen Arbeitsgeräten.
Aktualität	Betriebssysteme und Anwendungen werden laufend mit Sicherheitsaktualisierungen versorgt.
Netzabsicherung	Keine selbst betriebenen, aus dem Internet erreichbaren Systeme. Der Schutz der zugrunde liegenden Cloud- und Netzwerkinfrastruktur wird durch die eingesetzten Anbieter gewährleistet. Der Auftragsverarbeiter bleibt für die sichere Auswahl, Konfiguration und Nutzung dieser Dienste sowie für die Sicherheit der eigenen Anwendung verantwortlich.

Zugangskontrolle (Anwendung, Seite des Verantwortlichen)

Maßnahme	Umsetzung
Anmeldung	E-Mail und Passwort, Verifizierung der E-Mail-Adresse verpflichtend.
Passwortspeicherung	Ausschließlich als kryptographischer Hash.
Sitzungen	Zeitlich begrenzt; Zugriff auf Dateien nur über kurzlebige, signierte Verweise nach Anmeldung.

Zugriffskontrolle

Maßnahme	Umsetzung
Produktivzugriff	**Ausschließlich ein Mitglied der Geschäftsführung.** Es bestehen keine weiteren Konten mit Zugriff auf Produktivdaten.
Personalisierte Konten	Kein Sammel- oder Funktionskonto; jeder Zugriff ist einer natürlichen Person zugeordnet.
Rollenmodell	Innerhalb eines Mandanten Administrator und Buchhalter mit abgestuften Rechten.
Datenbankrechte	Rollenbasiert; Zugriff über Zeilensicherheitsregeln erzwungen.
Grundsatz	Zugriff nur, soweit für die Aufgabe erforderlich.
Zugriff auf Sicherungen	Ausschließlich dasselbe Mitglied der Geschäftsführung. Es bestehen keine weiteren Konten mit Zugriff auf Sicherungen oder auf deren Wiederherstellung.
Protokollierung	Zugriffe im Rahmen der Supportfunktion, Zugriffe auf hinterlegte Zugangsdaten sowie Importe und Exporte werden protokolliert.

Trennungskontrolle

Maßnahme	Umsetzung
Mandantentrennung	Auf Datenbankebene durch Zeilensicherheitsregeln (Row Level Security) je Mandant sowie getrennte Pfade im Dateispeicher. Jede Tabelle führt die Mandantenkennung.

Umgebungen	Produktiv- und Entwicklungsumgebung sind getrennt.
Zwecktrennung	Abrechnungsdaten, Belegdaten und Supportvorgänge werden in getrennten Datenbeständen geführt.

2. Integrität

Maßnahme	Umsetzung
Übertragung	Durchgehend TLS 1.2 oder höher; HSTS aktiv. Keine unverschlüsselte Übertragung personenbezogener Daten.
Inhaltssicherheit	Content Security Policy aktiv; Sicherheitskopfzeilen gesetzt.
Dateiablage	Nicht-öffentliche Speicherbereiche; kein direkter Zugriff ohne Anmeldung.
Verschlüsselung im Ruhezustand	Datenbank und Dateispeicher werden vom Anbieter im Ruhezustand verschlüsselt gespeichert.
Hinterlegte Zugangsdaten	Zugangsdaten zu Postfächern, Lieferantenportalen und Zahlungsdiensten werden zusätzlich mit AES-256-GCM verschlüsselt; der Schlüssel wird getrennt von der Datenbank verwahrt. Klartext entsteht nur bei der Verwendung bzw. beim protokollierten Abruf im Rahmen der Einrichtung.
Eingabekontrolle	Belegeingang, Importe und Exporte werden mit Zeitpunkt protokolliert. Kassabuch-Korrekturen ausschließlich als Stornobuchung mit Begründung und Bezug auf die ursprüngliche Buchung.
Unveränderbarkeit von Belegen	Keine Funktion zum Ersetzen oder Bearbeiten des Inhalts einer abgelegten Datei.

3. Verfügbarkeit und Belastbarkeit

Maßnahme	Umsetzung
Sicherung der Datenbank	Täglich automatisch, Aufbewahrung sieben Tage.
Belegdateien	Redundante Ablage im Rechenzentrum. **Die Datenbanksicherung umfasst die Dateien nicht.**
Zusätzliche Off-Site-Sicherung	**In Umsetzung**, noch nicht in Betrieb.
Wiederherstellung	Aus der Datenbanksicherung möglich.
Überwachung	Automatisierte Prüfung der Eingangskanäle mit Alarmierung per E-Mail bei Ausfall.

4. Verfahren zur regelmäßigen Überprüfung

Maßnahme	Umsetzung
Verzeichnis der Verarbeitungstätigkeiten	Vorhanden und laufend gepflegt.

Nachführung der Dokumentation	Die Datenschutzdokumentation wird gemeinsam mit der Produktänderung geführt und in derselben Versionsverwaltung abgelegt. Jede Änderung ist über die Versionsgeschichte mit Datum, Anlass und Umfang nachvollziehbar.
Auftragsverarbeiter	Werden vor Beauftragung auf ihre Maßnahmen geprüft und während der Zusammenarbeit regelmäßig bewertet; Grundlage sind deren Zertifizierungen und Prüfberichte.
Auftragsverarbeitungsverträge	Mit den eingesetzten Anbietern abgeschlossen und dokumentiert.
Vertraulichkeit der handelnden Personen	Verpflichtung auf das Datengeheimnis in Textform; die Liste der verpflichteten Personen wird geführt.
Umgang mit Datenschutzvorfällen	Dokumentierter Ablauf mit Fristen, Zuständigkeit und Vorfallsregister.
Drittlandübermittlung	Nur auf Grundlage von Standardvertragsklauseln, des EU-US-Datenschutzrahmens oder eines Angemessenheitsbeschlusses.

5. Datensparsamkeit und maschinelle Auslesung

Maßnahme	Umsetzung
Ergebnisse der Auslesung	Werden ausschließlich als strukturierte Felder gespeichert; Rohdaten der Auslesung werden nicht vorgehalten.
Eingehende E-Mails	Werden nach der Verarbeitung nicht dauerhaft gespeichert.
Verarbeitungsort der Auslesung	Rechenzentren von Amazon Web Services in der Europäischen Union. Die Anfrage geht an die Region Frankfurt am Main; verarbeitet wird je nach Auslastung in Deutschland, Schweden, Italien, Spanien, Irland oder Frankreich. Eine Verarbeitung außerhalb der EU findet nicht statt.
Modellanbieter	Erhält die übermittelten Dateien nicht.
Training	Die Eingaben werden nicht zu Trainingszwecken verwendet.

6. Löschung

Maßnahme	Umsetzung
Fristen	Festgelegt in Ziffer 6 der Allgemeinen Geschäftsbedingungen und in § 11 dieses Vertrags: 60 Tage nach Ablauf des bezahlten Zeitraums bzw. 60 Tage nach Registrierung ohne Abonnement.
Sicherungen	Datenbanksicherungen werden sieben Tage vorgehalten; gelöschte Daten verfallen mit dem Sicherungsstand.
Vernichtung von Datenträgern	Nicht einschlägig – es werden keine physischen Datenträger mit Daten des Verantwortlichen verarbeitet.

7. Nicht einschlägige Maßnahmen

Die folgenden in Prüfkatalogen üblichen Punkte treffen auf das Verfahren nicht zu und werden daher nicht geführt:

- **Kennzeichnung und Verwaltung von Datenträgern des Auftraggebers** – es werden keine physischen Datenträger übernommen.
- **Getrennte Aufbewahrung primärer Identifikationsmerkmale** – die Belege müssen urschriftgetreu wiedergegeben werden; eine Trennung von Namen und Belegbild würde diesem Zweck widersprechen.
- **Pseudonymisierung der Belegdaten** – für den Verarbeitungszweck nicht geeignet, da der Beleg einschließlich der gesetzlich erforderlichen Rechnungsmerkmale vollständig verarbeitet und wiedergegeben werden muss (§ 11 UStG; hinsichtlich der Aufbewahrung § 132 BAO).
- **Besucherregelung und Schlüsselvergabe für Geschäftsräume** – es besteht kein Publikumsverkehr; sämtliche Tätigkeiten erfolgen im Homeoffice.

8. Offene Punkte

Zur ehrlichen Einordnung – diese Maßnahme ist derzeit **nicht** umgesetzt:

1. **Zusätzliche Sicherung der Belegdateien außerhalb des Rechenzentrums** (siehe Abschnitt 3). Befindet sich in Entwicklung. Bis zur Inbetriebnahme sind die Belegdateien ausschließlich im Rechenzentrum Frankfurt am Main vorhanden und von der Datenbanksicherung nicht umfasst.

Anlage 3 – Unterauftragsverarbeiter

Stand: 06.10.2026

Anbieter	Sitz	Zweck	Verarbeitungsort	Grundlage bei Drittlandbezug
Supabase Pte. Ltd., Singapur	Singapur	Datenbank, Anmeldung, Dateispeicher	Frankfurt am Main	Standardvertragsklauseln
Vercel Inc.	USA	Betrieb der Anwendung	Frankfurt am Main für die serverseitige Ausführung; vorgelagertes weltweites Auslieferungsnetz (CDN) und weitere technische Verarbeitung durch Vercel möglich	Standardvertragsklauseln
Amazon Web Services EMEA SARL („AWS Europe“), 38 Avenue John F. Kennedy, L-1855 Luxemburg	Luxemburg	Maschinelle Belegauslesung, Hilfe-Assistent und Antwortentwürfe im Support (Amazon Bedrock)	EU – Anfrage über Frankfurt am Main, Verarbeitung in Deutschland, Schweden, Italien, Spanien, Irland oder Frankreich	–

AC PM LLC (Postmark), Chicago	USA	Belegeingang über die zentrale E-Mail-Adresse	USA	EU-US-Datenschutzrahmen, ergänzend Standardvertragsklauseln
Plus Five Five, Inc. (Resend)	USA	Versand transaktionaler E-Mails	USA (Speicherung und Verarbeitung); der Versand kann über eine EU-Senderegion erfolgen	Standardvertragsklauseln, ergänzend EU-US-Datenschutzrahmen
SuperX GmbH (Superchat), Prenzlauer Allee 242–247, 10405 Berlin	Deutschland	Belegeingang über WhatsApp (optional)	Deutschland	–
360dialog GmbH	Deutschland	Anbindung an die WhatsApp-Business-Schnittstelle (Unterauftragnehmer der SuperX GmbH)	EU	–
Meta Platforms Ireland Ltd.	Irland	Zustellung der WhatsApp-Nachrichten (Unterauftragnehmer der SuperX GmbH)	Frankfurt am Main; Verkehrsdaten USA	Standardvertragsklauseln
Microsoft Ireland Operations Limited	Irland	Anbindung des Mandanten-Postfachs und Belegeingang über OneDrive (optional)	EU	–
Google LLC	USA	Anbindung des Mandanten-Postfachs über die Gmail-Schnittstelle (optional)	EU (Postfach des Endnutzers); Schnittstellennutzung nach den Google-API-Bedingungen	EU-US-Datenschutzrahmen, ergänzend Standardvertragsklauseln
fino data services GmbH (GetMyInvoices), Universitätsplatz 12, 34127 Kassel	Deutschland	Abruf von Rechnungen aus Lieferantenportalen (optional)	Deutschland; eigene Unterauftragnehmer teils in den USA	Standardvertragsklauseln

Keine Unterauftragsverarbeiter sind Dienste, die der Verantwortliche selbst anbindet und die als Quelle oder Ziel seiner eigenen Daten dienen – etwa sein PayPal- oder Stripe-Konto oder die Buchhaltungssoftware seiner Steuerberatung. Mit diesen Anbietern steht er selbst in einem Vertragsverhältnis.

Kontoumsatzabruf. Der optionale automatische Abruf von Kontoumsätzen erfolgt über die BANKSapi Technology GmbH, Pettenkoferstraße 35, 80336 München, als nach dem Zahlungsdienstegesetz zugelassenen Kontoinformationsdienst. Der Verantwortliche erteilt die Zustimmung zum Abruf gegenüber seiner Bank selbst; BANKSapi handelt dabei eigenverantwortlich und ist kein Unterauftragsverarbeiter im Sinne dieses Vertrags. Die abgerufenen Umsätze verarbeitet der Auftragsverarbeiter anschließend im Auftrag des Verantwortlichen.

Optionale Dienste. WhatsApp-Belegeingang, Postfachanbindung und Portalabruf werden nur wirksam, wenn der Verantwortliche sie aktiviert. Wird ein Dienst nicht genutzt, findet über ihn keine Verarbeitung statt.

Hinweis zur Gmail-Anbindung. Das Postfach des Verantwortlichen wird von dessen eigenem Anbieter betrieben – im Europäischen Wirtschaftsraum regelmäßig die Google Ireland Limited. Vertragspartner für die Nutzung der Schnittstelle, über die der Auftragsverarbeiter das Postfach abruft, ist nach den Google-API-Bedingungen dagegen die Google LLC mit Sitz in den Vereinigten Staaten. Die Anbindung ist optional. Entsprechendes gilt für ein Postfach bei Microsoft: Es wird unter dem eigenen Vertrag des Verantwortlichen mit seinem Anbieter betrieben; die Nennung von Google LLC und Microsoft in dieser Anlage dient der vollständigen Offenlegung.

Hinweis zur zentralen E-Mail-Adresse. Belege, die an die zentrale Eingangsadresse des Auftragsverarbeiters gesendet werden, nimmt ein Dienstleister mit Sitz in den Vereinigten Staaten entgegen und reicht sie weiter. Bindet der Verantwortliche stattdessen sein eigenes Postfach an oder nutzt Upload, WhatsApp oder den Portalabruf, entfällt dieser Weg.