Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Anlage zum Nutzungsvertrag über die Software myERP24

VERANTWORTLICHER („KUNDE“)
[Firma, Rechtsform]
[Straße, Hausnummer]
[PLZ Ort]
vertreten durch: [Name, Funktion]
Datenschutzkontakt: [E-Mail]

AUFTRAGSVERARBEITER („RIEBOTEC“)
riebotec UG (haftungsbeschränkt)
Martin-Luther-Straße 15
42285 Wuppertal, Deutschland
vertreten durch: [Geschäftsführer/in]
Datenschutzkontakt: anfragen@myerp24.de

Präambel

Der Kunde nutzt die von riebotec als Software-as-a-Service bereitgestellte Anwendung myERP24 („Software“) auf Grundlage der Allgemeinen Geschäftsbedingungen und des Nutzungsvertrags („Hauptvertrag“). Im Rahmen der Nutzung verarbeitet riebotec personenbezogene Daten im Auftrag des Kunden, insbesondere Stamm-, Vorgangs-, Beleg- und Buchungsdaten des Kunden sowie Daten seiner Kunden, Lieferanten und Mitarbeitenden. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 Abs. 3 DSGVO. Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in datenschutzrechtlichen Fragen vor.

§ 1 Gegenstand, Dauer und Konkretisierung

(1) Gegenstand der Verarbeitung ist der Betrieb der Software für den Kunden einschließlich Hosting, Datensicherung, Wartung, Support und der in Anlage 1 beschriebenen Funktionen (u. a. Belegerkennung, Bankabruf, E-Rechnungs-Postfach, DATEV-Export, Steuerformulare, KI-Assistenten).

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

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Die Pflichten aus § 10 (Löschung und Rückgabe) bestehen darüber hinaus bis zu ihrer vollständigen Erfüllung.

(4) Die Verarbeitung findet ausschließlich in Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums statt. Das produktive Hosting erfolgt in einem Rechenzentrum in Deutschland (Anlage 3). Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Kunden in Textform und setzt die Einhaltung der Art. 44 ff. DSGVO voraus.

§ 2 Weisungsgebundenheit

(1) riebotec verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und auf dokumentierte Weisung des Kunden, sofern riebotec nicht durch das Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet ist; in diesem Fall teilt riebotec dem

Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Hauptvertrag, dieser Vertrag und die Nutzung der Funktionen der Software durch den Kunden (einschließlich der von ihm oder seinen Nutzern vorgenommenen Einstellungen und ausgelösten Verarbeitungen) gelten als Gesamtheit der dokumentierten Weisungen. Einzelweisungen erteilt der Kunde in Textform an anfragen@myerp24.de oder über die in der Software bereitgestellte Supportfunktion; mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Weisungsberechtigt sind die in der Software als Administrator hinterlegten Personen des Kunden. Änderungen teilt der Kunde unverzüglich mit.

(4) Hält riebotec eine Weisung für rechtswidrig, informiert riebotec den Kunden unverzüglich und ist berechtigt, die Ausführung bis zur Bestätigung oder Änderung der Weisung auszusetzen.

(5) Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, können gesondert vergütungspflichtig sein; riebotec weist hierauf vor Ausführung hin.

§ 3 Pflichten und Verantwortung des Kunden

(1) Der Kunde ist im Rahmen dieses Vertrags Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist allein verantwortlich für die Rechtmäßigkeit der Datenerhebung, der Verarbeitung und der Übermittlung an riebotec sowie für die Wahrung der Rechte der betroffenen Personen, einschließlich der Informationspflichten nach Art. 13 und 14 DSGVO.

(2) Der Kunde ist für die Einhaltung der ihn treffenden handels- und steuerrechtlichen Pflichten verantwortlich, insbesondere nach § 147 AO, § 257 HGB und den GoBD. riebotec unterstützt ihn hierbei durch die in Anlage 1 beschriebenen Funktionen (revisionssichere Ablage, Verfahrensdokumentation, Z3-/GoBD-Export, DATEV-Export).

(3) Der Kunde stellt sicher, dass nur solche Daten in die Software eingegeben werden, zu deren Verarbeitung er berechtigt ist, und dass Zugänge, Rollen und Rechte in der Software seinem Berechtigungskonzept entsprechen.

(4) Der Kunde informiert riebotec unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Verarbeitungsergebnisse feststellt.

§ 4 Pflichten von riebotec

(1) riebotec verarbeitet Daten nur im Rahmen des Auftrags und der Weisungen des Kunden. Eine Verarbeitung zu eigenen Zwecken ist ausgeschlossen, soweit nicht § 11 dieses Vertrags ausdrücklich etwas anderes bestimmt.

(2) riebotec gewährleistet, dass die mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO), und dass sie vor Aufnahme der Tätigkeit mit den einschlägigen

Datenschutzbestimmungen vertraut gemacht wurden. Die Vertraulichkeitspflicht besteht auch nach Beendigung der Tätigkeit fort.

(3) riebotec hat – soweit gesetzlich erforderlich – eine Datenschutzbeauftragte Person benannt: [Name/„nicht erforderlich“]. riebotec benennt einen fachlich verantwortlichen Ansprechpartner für Datenschutz: anfragen@myerp24.de.

(4) riebotec unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(5) riebotec führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dem Kunden den ihn betreffenden Auszug auf Anfrage zur Verfügung.

(6) riebotec stellt sicher, dass Produktivdaten des Kunden strikt mandantengetrennt verarbeitet werden und dass Zugriffe von riebotec-Mitarbeitenden auf Produktivdaten (z. B. im Support) protokolliert werden und nur mit Freigabe des Kunden über die Supportfunktion erfolgen.

§ 5 Technische und organisatorische Maßnahmen

(1) riebotec trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Die Maßnahmen gewährleisten unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umständen und Zwecken der Verarbeitung ein dem Risiko angemessenes Schutzniveau hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. riebotec darf alternative Maßnahmen umsetzen, sofern das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert und dem Kunden auf Anfrage mitgeteilt.

(3) riebotec überprüft die Wirksamkeit der Maßnahmen regelmäßig, mindestens jährlich, und dokumentiert das Ergebnis.

§ 6 Unterauftragsverhältnisse

(1) Der Kunde erteilt riebotec die allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und gelten als genehmigt.

(2) riebotec informiert den Kunden mindestens vier Wochen vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform (E-Mail an die Administratoren und Hinweis in der Software). Der Kunde kann der Änderung innerhalb von vier Wochen aus wichtigem datenschutzrechtlichem Grund widersprechen. Widerspricht der Kunde und kann keine einvernehmliche Lösung gefunden werden, steht beiden Parteien ein Sonderkündigungsrecht für den Hauptvertrag zum Zeitpunkt der beabsichtigten Änderung zu.

(3) riebotec erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet riebotec gegenüber dem Kunden für die Einhaltung der Pflichten dieses Unterauftragsverarbeiters.

(4) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen wie Telekommunikation, Post-/Transportdienste, Reinigung oder Wartung ohne Datenzugriff. riebotec stellt auch hier angemessene Vertraulichkeit sicher.

§ 7 Rechte der betroffenen Personen

(1) riebotec unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte (Art. 12 bis 22 DSGVO) nachzukommen, insbesondere durch Export-, Berichtigungs-, Sperr- und Anonymisierungsfunktionen in der Software.

(2) Wendet sich eine betroffene Person unmittelbar an riebotec, leitet riebotec das Ersuchen unverzüglich an den Kunden weiter und antwortet der betroffenen Person nicht in der Sache, sondern verweist auf den Kunden, soweit nicht gesetzlich etwas anderes geboten ist.

(3) Löschungen aufbewahrungspflichtiger Belege und Buchungen erfolgen gemäß den gesetzlichen Fristen durch Anonymisierung der personenbezogenen Angaben bei Erhalt des buchungsrelevanten Inhalts („Anonymisieren statt Löschen“); der Kunde löst diese Funktion in der Software eigenverantwortlich aus.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) riebotec meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten, die Daten des Kunden betrifft, unverzüglich, spätestens innerhalb von 36 Stunden nach Bekanntwerden, an die hinterlegten Administratoren und den Datenschutzkontakt des Kunden.

(2) Die Meldung enthält, soweit bereits bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, betroffene Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen. Nachträglich bekannt werdende Informationen werden unverzüglich nachgereicht.

(3) riebotec unterstützt den Kunden bei der Erfüllung seiner Melde- und Benachrichtigungspflichten gegenüber Aufsichtsbehörden und betroffenen Personen (Art. 33, 34 DSGVO). Die Entscheidung über Meldungen trifft der Kunde.

(4) riebotec dokumentiert alle Verletzungen einschließlich ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen.

Entwurf zur anwaltlichen Prüfung. Keine Rechtsberatung. Verbindlich ist ausschließlich die von beiden Parteien unterzeichnete Fassung.

§ 9 Nachweise und Kontrollrechte

(1) riebotec stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO zur Verfügung, insbesondere die aktuelle Fassung der Anlage 2, Prüfberichte, Zertifizierungen oder Selbstauskünfte.

(2) Der Kunde ist berechtigt, die Einhaltung dieses Vertrags einmal jährlich sowie anlassbezogen zu überprüfen – vorrangig durch Einsichtnahme in die nach Abs. 1 bereitgestellten Unterlagen. Genügen diese nicht, kann der Kunde nach Ankündigung mit angemessener Frist (in der Regel 14 Tage) zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs eine Vor-Ort-Kontrolle selbst oder durch einen zur Verschwiegenheit verpflichteten Dritten durchführen lassen. riebotec kann die Beauftragung eines Wettbewerbers ablehnen.

(3) Den Aufwand für Kontrollen, die über die Bereitstellung von Unterlagen nach Abs. 1 hinausgehen und nicht durch Anhaltspunkte für Verstöße von riebotec veranlasst sind, kann riebotec nach seiner jeweils gültigen Preisliste berechnen.

(4) riebotec informiert den Kunden unverzüglich über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, soweit diese sich auf die Verarbeitung der Daten des Kunden beziehen.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Nach Beendigung des Hauptvertrags stellt riebotec dem Kunden sämtliche in der Software gespeicherten Daten für die Dauer von 60 Tagen zum Export zur Verfügung: Stamm- und Vorgangsdaten in maschinenlesbaren Formaten (CSV), Belege und Dokumente als PDF/Original, Buchungen als DATEV-Export (EXTF) und GoBD-Export (Z3) einschließlich der Verfahrensdokumentation. In diesem Zeitraum ist die Software im Lesemodus nutzbar.

(2) Nach Ablauf der Frist löscht riebotec alle Daten des Kunden einschließlich Kopien, Datensicherungen (nach Ablauf der Backup-Rotation von höchstens 90 Tagen) und Protokolle, soweit keine gesetzliche Aufbewahrungspflicht von riebotec entgegensteht. Die Löschung wird dem Kunden auf Anfrage schriftlich bestätigt.

(3) Auf Wunsch des Kunden kann riebotec gegen gesonderte Vergütung einen verlängerten Lesezugriff („Archivzugang“) bereitstellen, um die Aufbewahrungspflichten des Kunden zu unterstützen. Die Verantwortung für die Aufbewahrung verbleibt beim Kunden.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, darf riebotec entsprechend den gesetzlichen Fristen über das Vertragsende hinaus aufbewahren.

Entwurf zur anwaltlichen Prüfung. Keine Rechtsberatung. Verbindlich ist ausschließlich die von beiden Parteien unterzeichnete Fassung.

§ 11 Nutzung von Daten zur Produktverbesserung (eigener Zweck)

> Dieser Paragraf regelt eine Verarbeitung, die **nicht** Teil der Auftragsverarbeitung ist. Soweit riebotec Daten zur Verbesserung der Software für alle Kunden nutzt, verfolgt riebotec einen eigenen Zweck und ist insoweit selbst Verantwortlicher (Art. 4 Nr. 7, Art. 28 Abs. 10 DSGVO). Die Regelung trennt diese Verarbeitung klar von der Auftragsverarbeitung und knüpft sie an eine jederzeit widerrufliche Freigabe des Kunden.

(1) Anonymisierte Nutzung ohne Freigabe. riebotec ist berechtigt, Daten aus der Nutzung der Software in vollständig anonymisierter und aggregierter Form zu verwenden, um die Software zu betreiben, zu sichern, zu analysieren und weiterzuentwickeln (z. B. Nutzungsstatistiken, Fehler- und Leistungsmetriken, Häufigkeit von Funktionsaufrufen). Anonymisiert sind Daten nur, wenn eine Re-Identifizierung betroffener Personen oder des Kunden nach dem Stand der Technik mit verhältnismäßigem Aufwand ausgeschlossen ist. Solche Daten unterliegen nicht der DSGVO.

(2) Freigabe zur Produktverbesserung („Beitrag zur Produktverbesserung“). Darüber hinaus kann der Kunde riebotec gestatten, Buchungs- und Belegdaten des Kunden zur Verbesserung der KI-Assistenten und der Belegerkennung für alle Kunden zu verwenden, insbesondere zum Training und zur Validierung von Modellen für Kontierungs-, Steuersatz- und Kennzahlenvorschläge sowie zur Erkennung von Belegstrukturen. Die Freigabe ist **standardmäßig deaktiviert** (Opt-in) und wird vom Kunden ausschließlich durch einen Administrator über die Programmoberfläche unter *Administration → Datenschutz → Beitrag zur Produktverbesserung* erteilt. Die Erteilung wird mit Zeitpunkt, Benutzer und Versionsstand dieser Regelung protokolliert.

(3) Umfang und Schutzmaßnahmen. Für die Verarbeitung nach Abs. 2 gilt:

- Verarbeitet werden nur Buchungszeilen, Kontenzuordnungen, Steuersätze, Belegstrukturmerkmale und Kennzahlenzuordnungen. Freitextfelder, Namen natürlicher Personen, Bankverbindungen, Personalakten, Tresordaten und Dokumente der Mitarbeitenden sind ausgeschlossen.
- Vor der Verwendung werden die Daten pseudonymisiert: Geschäftspartner werden durch Tokens ersetzt, Beträge gerundet oder in Klassen überführt, Mandantenkennungen entfernt. Der Schlüssel verbleibt im Mandanten des Kunden.
- Die Verarbeitung erfolgt ausschließlich in der EU; eine Übermittlung an Dritte außerhalb der in Anlage 3 genannten Unterauftragsverarbeiter findet nicht statt. Daten werden nicht an Anbieter externer KI-Modelle zu deren eigenen Trainingszwecken weitergegeben.
- Trainierte Modelle enthalten keine wiederherstellbaren Einzeldaten des Kunden. riebotec prüft dies vor jeder Freigabe eines Modells (Memorisierungs- und Extraktionstest) und dokumentiert das Ergebnis.
- riebotec verwendet die Daten nicht zur Bewertung einzelner Kunden, Geschäftspartner oder Personen, nicht zu Werbezwecken und nicht für den Verkauf an Dritte.

(4) Rechtsgrundlage und Rollenverteilung. Für die Verarbeitung nach Abs. 2 ist riebotec Verantwortlicher. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Verbesserung der Software zugunsten aller Kunden) in Verbindung mit der Freigabe des Kunden; soweit der Kunde Daten natürlicher Personen einbringt, stellt er sicher, dass die betroffenen Personen

gemäß Art. 13/14 DSGVO über die Weitergabe an riebotec zu diesem Zweck informiert sind. riebotec stellt hierfür einen Textbaustein in der Software bereit. Die Parteien sind sich einig, dass keine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO begründet wird.

(5) Widerruf. Der Kunde kann die Freigabe **jederzeit mit Wirkung für die Zukunft** widerrufen – über dieselbe Programmoberfläche (*Administration → Datenschutz → Beitrag zur Produktverbesserung → Deaktivieren*) oder in Textform an anfragen@myerp24.de. Mit dem Widerruf stellt riebotec die weitere Verwendung der Daten des Kunden für Trainingszwecke unverzüglich, spätestens innerhalb von 72 Stunden, ein und löscht noch nicht verarbeitete Rohdaten aus den Trainingsvorräten. Bereits trainierte Modelle bleiben unberührt, sofern sie nach Abs. 3 keine Einzeldaten des Kunden enthalten; andernfalls wird das Modell zurückgezogen. Der Widerruf hat keine Auswirkung auf die Nutzbarkeit der Software oder deren Preis.

(6) Hinweis in der Software. riebotec informiert über den Status der Freigabe dauerhaft sichtbar in der Programmoberfläche und weist bei jeder Aktivierung auf die Widerrufsmöglichkeit, den Umfang nach Abs. 3 und die Informationspflicht nach Abs. 4 hin. Änderungen dieses Paragrafen werden dem Kunden mindestens sechs Wochen vor Wirksamwerden mitgeteilt; eine erteilte Freigabe erlischt bei einer Erweiterung des Umfangs und muss erneut erteilt werden.

(7) Lokale Lernmodelle. Unberührt bleibt das Lernen der KI-Assistenten im Browser des Kunden ausschließlich aus dessen eigenen, freigegebenen Buchungen. Diese Modelle verbleiben im Mandanten des Kunden und sind Teil der Auftragsverarbeitung.

§ 12 Haftung

(1) Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für den Schaden, der durch eine ihr zurechnebare Verletzung der DSGVO oder dieses Vertrags verursacht wurde; die Parteien stellen sich insoweit wechselseitig frei.

(2) Im Übrigen gelten die Haftungsregelungen des Hauptvertrags, soweit zwingendes Recht nichts anderes bestimmt.

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Textformerfordernisses.

(2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit des Vertrags im Übrigen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die dem Zweck der Verordnung am nächsten kommt.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Wuppertal, soweit der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

(4) Dieser Vertrag kann elektronisch durch Annahme in der Programmoberfläche durch einen Administrator des Kunden geschlossen werden; riebotec stellt die angenommene Fassung als PDF mit Zeitstempel bereit. Alternativ gilt die unterzeichnete Fassung.

Ort, Datum · Kunde (Verantwortlicher)

Ort, Datum · riebotec UG (haftungsbeschränkt)

Entwurf zur anwaltlichen Prüfung. Keine Rechtsberatung. Verbindlich ist ausschließlich die von beiden Parteien unterzeichnete Fassung.

Anlage 1 – Gegenstand, Daten, betroffene Personen

1. Art und Zweck der Verarbeitung

Bereitstellung und Betrieb der Software myERP24 als Mandanteninstanz: Speicherung, Verarbeitung, Anzeige, Export und Sicherung der vom Kunden eingegebenen oder importierten Daten; automatisierte Verarbeitungen im Auftrag: Belegerkennung (OCR, XRechnung/ZUGFeRD-Auswertung), Bankabruf und Zahlungsabgleich (FinTS/Import), E-Rechnungs-Postfach, Buchungsvorschläge und Steuerkennzahlenzuordnung durch KI-Assistenten (Freigabe durch den Kunden), DATEV-/GoBD-Export, Erzeugung von Steuerformular-Arbeitsblättern, Synchronisation mit Microsoft 365 (sofern vom Kunden eingerichtet), Support und Fehleranalyse.

2. Kategorien personenbezogener Daten

Kategorie	Beispiele
Stammdaten Geschäftspartner	Name, Anschrift, Kontaktdaten, USt-IdNr., Konditionen, Bankverbindung (IBAN), Kunden-/Lieferantennummer
Ansprechpartner	Name, Funktion, Telefon, E-Mail, Kommunikationsverlauf
Objekt- und Vorgangsdaten	Adressen, Fotos von Objekten, Aufgaben, Termine, Checklisten, Leistungsberichte
Beleg- und Buchungsdaten	Angebote, Aufträge, Rechnungen, Eingangsrechnungen, Kontoauszüge, Buchungen, offene Posten, Mahnungen, Steuerkennzahlen
Mitarbeiterdaten des Kunden	Name, Rolle, Login, Signatur, Arbeitszeiten, Postfachzuordnung; Personalakte (Verträge, Ausweise, Zertifikate – verschlüsselt im Datentresor)
Nutzungs- und Protokolldaten	Anmeldungen, Audit-Trail, IP-Adresse, Zeitstempel, Änderungsprotokolle
Besondere Kategorien (Art. 9)	Nicht vorgesehen; können in Personalakten enthalten sein (z. B. Schwerbehinderung) – nur verschlüsselt im Datentresor, ohne Auswertung durch riebotec

3. Kategorien betroffener Personen

Kunden, Lieferanten und deren Ansprechpartner; Interessenten; Mitarbeitende und Auftragnehmer des Kunden; Nutzer der Software; Steuerberater und sonstige vom Kunden einbezogene Dritte.

Entwurf zur anwaltlichen Prüfung. Keine Rechtsberatung. Verbindlich ist ausschließlich die von beiden Parteien unterzeichnete Fassung.

Anlage 2 – Technische und organisatorische

Entwurf zur anwaltlichen Prüfung. Keine Rechtsberatung. Verbindlich ist ausschließlich die von beiden Parteien unterzeichnete Fassung.

Maßnahmen (Art. 32 DSGVO)

Bereich	Maßnahmen
Vertraulichkeit – Zutritt	Rechenzentrum in Deutschland mit Zutrittskontrolle, Videoüberwachung, Besucherregelung; riebotec-Büro mit Schließsystem; keine Produktivdaten auf mobilen Datenträgern.
Vertraulichkeit – Zugang	Individuelle Benutzerkonten, Passwortrichtlinie, Mehrfaktor-Authentifizierung für Administratoren und riebotec-Personal, Sperre nach Fehlversuchen, Sitzungs-Timeout, Wartungsmodus, Registrierungs- und Passwort-Workflows mit Administratorfreigabe.
Vertraulichkeit – Zugriff	Rollenmatrix (User, Mitarbeiter, Koordinator, Desktop-Nutzer, Administrator) und Rechteprofile, serverseitige Prüfung jeder Funktion; Vier-Augen-Prinzip bei Freigaben; Supportzugriff nur nach Freigabe des Kunden, protokolliert; Secrets ausschließlich in geschützter Konfiguration (Konfigurationszentrum mit Allowlist), nie im Browser.
Vertraulichkeit – Trennung	Logische Mandantentrennung auf Datenbank- und Dateiebene; getrennte Umgebungen für Entwicklung, Test und Produktion; Testdaten synthetisch oder anonymisiert.
Pseudonymisierung / Verschlüsselung	TLS 1.2+ für jede Übertragung; Datentresor mit AES-256-GCM für Zugangsdaten, Bankzugänge, Personalakten und Zertifikate, Schlüsselrotation, Zugriffsprotokoll; verschlüsselte Datensicherungen; Pseudonymisierung vor jeder Verwendung nach § 11 Abs. 2.
Integrität – Eingabe/ Änderung	Unveränderliches Buchungsjournal; festgeschriebene Belege unveränderbar, PDF mit SHA-256 archiviert; Audit-Trail für jede Änderung mit Benutzer und Zeitstempel; Versionierung von Vorlagen.
Integrität – Weitergabe	Schnittstellen (FinTS, Microsoft Graph, KI-API, E-Rechnungs-Postfach) mit minimalen Berechtigungen, Healthchecks, Statusausweis je Integration; Übertragung an die KI-API nur pseudonymisiert und ohne Beträge/Geschäftspartner (§ 11); signierter Support-Ticket-Eingang mit Duplikatschutz.
Verfügbarkeit und Belastbarkeit	Tägliche Datensicherung, Aufbewahrung 30 Tage rollierend (max. 90 Tage), geografisch getrennte Kopie in Deutschland; regelmäßige Wiederherstellungstests; Monitoring, Kapazitätsplanung, Lasttests; USV, Brandschutz und redundante Anbindung im Rechenzentrum; dokumentierter Notfall- und Rollback-Plan.
Verfahren zur Überprüfung	Datenschutzmanagement mit jährlicher Überprüfung der TOM; Incident-Response-Prozess mit 36-Stunden-Meldefrist; Änderungsmanagement mit Review, Test und Backup vor jedem Release; Schulung und Verpflichtung der Mitarbeitenden; Verzeichnis von Verarbeitungstätigkeiten.
Auftragskontrolle	Verarbeitung nur auf dokumentierte Weisung; Unterauftragsverarbeiter vertraglich gebunden und regelmäßig geprüft; Löschkonzept mit Nachweis; Aufbewahrungsfristen-Verwaltung (Anonymisieren statt Löschen).

Entwurf zur anwaltlichen Prüfung. Keine Rechtsberatung. Verbindlich ist ausschließlich die von beiden Parteien unterzeichnete Fassung.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung	Garantien
[Rechenzentrumsbetreiber, Anschrift]	Hosting, Infrastruktur, Datensicherung	Deutschland	AV-Vertrag, ISO 27001 [prüfen]
[Anbieter OCR-/KI-Dienst, Anschrift]	Texterkennung (Hybrid-OCR), KI-API-Infrastruktur	EU [Land]	AV-Vertrag, kein Training mit Kundendaten
[E-Mail-/Transaktionsdienst, Anschrift]	Versand von Systembenachrichtigungen	EU	AV-Vertrag
Microsoft Ireland Operations Ltd.	Microsoft 365 (nur, wenn der Kunde die Integration mit eigenem Tenant einrichtet – dann Vertragspartner des Kunden)	EU (EU Data Boundary)	Microsoft DPA des Kunden

Die aktuelle Liste ist jederzeit in der Software unter *Administration → Datenschutz → Unterauftragsverarbeiter* einsehbar. Änderungen werden nach § 6 Abs. 2 angekündigt.

Anlage 4 – Textbaustein für die Information betroffener Personen (zu § 11 Abs. 4)

„Zur Erstellung und Verwaltung unserer Geschäftsvorgänge nutzen wir die Software myERP24 der riebotec UG (haftungsbeschränkt), Wuppertal, die Ihre Daten in unserem Auftrag in Deutschland verarbeitet. Soweit wir dies freigegeben haben, verwendet riebotec Buchungs- und Belegstrukturdaten in pseudonymisierter Form zur Verbesserung ihrer Software (Art. 6 Abs. 1 lit. f DSGVO). Dabei werden keine Namen, Kontaktdaten oder Bankverbindungen verwendet. Weitere Informationen: www.myerp24.de/datenschutz.“

Der Kunde fügt diesen Baustein in seine Datenschutzinformationen gegenüber Geschäftspartnern und Mitarbeitenden ein, solange die Freigabe nach § 11 Abs. 2 aktiv ist.

Entwurf zur anwaltlichen Prüfung. Keine Rechtsberatung. Verbindlich ist ausschließlich die von beiden Parteien unterzeichnete Fassung.