Data Processing Agreement pursuant to Art. 28 GDPR

Annex to the subscription agreement for the myERP24 software

CONTROLLER ("CUSTOMER")

[Company, legal form]
[Street, number]
[Postcode, city]
represented by: [name, position]
Privacy contact: [e-mail]

PROCESSOR ("RIEBOTEC")

riebotec UG (haftungsbeschränkt)
Martin-Luther-Straße 15
42285 Wuppertal, Germany
represented by: [managing director]
Privacy contact: anfragen@myerp24.de

Preamble

The Customer uses the software-as-a-service application myERP24 ("Software") provided by riebotec on the basis of the General Terms and Conditions and the subscription agreement ("Main Agreement"). In the course of this use, riebotec processes personal data on behalf of the Customer, in particular master, case, document and posting data of the Customer as well as data of its customers, suppliers and employees. This Agreement specifies the parties' data protection obligations under Art. 28 (3) GDPR. In the event of conflict, this Agreement prevails over the Main Agreement in data protection matters.

§ 1 Subject matter, duration and specification

(1) The subject matter of processing is the operation of the Software for the Customer, including hosting, backup, maintenance, support and the functions described in Annex 1 (including document recognition, bank retrieval, e-invoice mailbox, DATEV export, tax forms, AI assistants).

(2) The nature and purpose of processing, the categories of personal data and the categories of data subjects are set out in Annex 1.

(3) The duration of processing corresponds to the term of the Main Agreement. The obligations under § 10 (deletion and return) continue until fully performed.

(4) Processing takes place exclusively in member states of the European Union or the European Economic Area. Production hosting is located in a data centre in Germany (Annex 3). Any relocation to a third country requires the Customer's prior consent in text form and compliance with Art. 44 et seq. GDPR.

§ 2 Processing on documented instructions

(1) riebotec processes personal data exclusively within the framework of the agreements made and on the Customer's documented instructions, unless riebotec is required to process by Union or Member State law; in that case riebotec informs the Customer of that legal requirement before processing,

unless the law prohibits such information on important grounds of public interest.

(2) The Main Agreement, this Agreement and the Customer's use of the Software's functions (including settings made and processing triggered by the Customer or its users) together constitute the documented instructions. Individual instructions are issued in text form to anfragen@myerp24.de or via the support function provided in the Software; oral instructions must be confirmed in text form without delay.

(3) Persons registered as administrators in the Software are authorised to issue instructions. The Customer notifies changes without delay.

(4) If riebotec considers an instruction to infringe the law, riebotec informs the Customer immediately and may suspend execution until the instruction is confirmed or amended.

(5) Instructions exceeding the agreed scope of services may be subject to separate remuneration; riebotec indicates this before execution.

§ 3 Obligations and responsibility of the Customer

(1) Under this Agreement the Customer is the controller within the meaning of Art. 4 (7) GDPR. The Customer is solely responsible for the lawfulness of data collection, processing and transfer to riebotec and for safeguarding data subjects' rights, including the information obligations under Art. 13 and 14 GDPR.

(2) The Customer is responsible for compliance with its commercial and tax law obligations, in particular under § 147 AO, § 257 HGB and the German GoBD principles. riebotec supports the Customer through the functions described in Annex 1 (audit-proof archive, process documentation, Z3/GoBD export, DATEV export).

(3) The Customer ensures that only data it is entitled to process is entered into the Software and that accesses, roles and permissions in the Software correspond to its authorisation concept.

(4) The Customer informs riebotec without delay if it detects errors or irregularities when checking the results of processing.

§ 4 Obligations of riebotec

(1) riebotec processes data only within the scope of the engagement and the Customer's instructions. Processing for riebotec's own purposes is excluded, unless § 11 of this Agreement expressly provides otherwise.

(2) riebotec ensures that persons engaged in processing have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28 (3) (b) GDPR) and have been familiarised with the relevant data protection provisions before commencing work. The confidentiality obligation survives the end of the engagement.

(3) Where legally required, riebotec has appointed a data protection officer: [name / “not required”]. riebotec designates a responsible contact for data protection: anfragen@myerp24.de.

(4) riebotec assists the Customer with appropriate technical and organisational measures in fulfilling its obligations under Art. 32 to 36 GDPR (security of processing, breach notification, data protection impact assessment, prior consultation).

(5) riebotec maintains a record of all categories of processing activities under Art. 30 (2) GDPR and provides the Customer with the relevant extract on request.

(6) riebotec ensures that the Customer's production data is processed with strict tenant separation and that access to production data by riebotec staff (e.g. in support) is logged and takes place only with the Customer's approval via the support function.

§ 5 Technical and organisational measures

(1) riebotec implements the technical and organisational measures described in Annex 2 pursuant to Art. 32 GDPR. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, the measures ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and resilience of the systems.

(2) The measures are subject to technical progress. riebotec may implement alternative measures provided the security level of the agreed measures is not undercut. Material changes are documented and communicated to the Customer on request.

(3) riebotec reviews the effectiveness of the measures regularly, at least annually, and documents the result.

§ 6 Sub-processors

(1) The Customer grants riebotec general authorisation to engage sub-processors. The sub-processors engaged at the time of conclusion are listed in Annex 3 and are deemed approved.

(2) riebotec informs the Customer at least four weeks before the intended engagement or replacement of a sub-processor in text form (e-mail to the administrators and notice in the Software). The Customer may object to the change within four weeks on important data protection grounds. If the Customer objects and no amicable solution is found, both parties have a special right to terminate the Main Agreement with effect from the intended change.

(3) riebotec imposes on each sub-processor by contract the same data protection obligations as set out in this Agreement, in particular sufficient guarantees of appropriate technical and organisational measures (Art. 28 (4) GDPR). Where a sub-processor fails to fulfil its obligations, riebotec remains liable to the Customer for the performance of that sub-processor's obligations.

(4) Ancillary services such as telecommunications, postal/transport services, cleaning or maintenance without data access are not sub-processing. riebotec ensures appropriate confidentiality here as well.

§ 7 Rights of data subjects

(1) riebotec assists the Customer with appropriate technical and organisational measures in fulfilling its obligation to respond to requests for exercising data subjects' rights (Art. 12 to 22 GDPR), in particular through export, rectification, blocking and anonymisation functions in the Software.

(2) If a data subject contacts riebotec directly, riebotec forwards the request to the Customer without delay and does not respond on the merits but refers the data subject to the Customer, unless otherwise required by law.

(3) Deletion of documents and postings subject to retention obligations is carried out in accordance with statutory periods by anonymising the personal details while preserving the accounting-relevant content (“anonymise instead of delete”); the Customer triggers this function in the Software on its own responsibility.

§ 8 Notification of personal data breaches

(1) riebotec notifies the Customer of any personal data breach affecting the Customer's data without undue delay, at the latest within 36 hours of becoming aware, to the registered administrators and the Customer's privacy contact.

(2) As far as already known, the notification contains the information under Art. 33 (3) GDPR: nature of the breach, categories and approximate number of data subjects and records concerned, likely consequences, measures taken and proposed. Information becoming known later is supplied without delay.

(3) riebotec assists the Customer in fulfilling its notification and communication obligations towards supervisory authorities and data subjects (Art. 33, 34 GDPR). The Customer decides on notifications.

(4) riebotec documents all breaches including their effects and the remedial action taken.

§ 9 Evidence and audit rights

(1) riebotec makes available to the Customer all information necessary to demonstrate compliance with the obligations under Art. 28 GDPR, in particular the current version of Annex 2, audit reports, certifications or self-assessments.

(2) The Customer may verify compliance with this Agreement once a year and on an ad-hoc basis where there is cause – primarily by reviewing the documents provided under para. 1. If these are insufficient, the Customer may, after notice with a reasonable period (usually 14 days), during normal business hours and without disrupting operations, carry out an on-site audit itself or through a third party bound to confidentiality. riebotec may refuse the appointment of a competitor.

(3) riebotec may charge, according to its current price list, for audits that go beyond the provision of documents under para. 1 and are not prompted by indications of breaches by riebotec.

(4) riebotec informs the Customer without delay of audits and measures by a supervisory authority insofar as they relate to the processing of the Customer's data.

§ 10 Deletion and return after the end of the agreement

(1) After termination of the Main Agreement, riebotec makes all data stored in the Software available to the Customer for export for 60 days: master and case data in machine-readable formats (CSV), documents as PDF/original, postings as DATEV export (EXTF) and GoBD export (Z3) including the process documentation. During this period the Software can be used in read-only mode.

(2) After expiry of the period, riebotec deletes all Customer data including copies, backups (after expiry of the backup rotation of at most 90 days) and logs, unless a statutory retention obligation of riebotec prevents this. Deletion is confirmed to the Customer in writing on request.

(3) At the Customer's request, riebotec may provide extended read access (“archive access”) against separate remuneration to support the Customer's retention obligations. Responsibility for retention remains with the Customer.

(4) riebotec may retain documentation serving as evidence of proper processing in accordance with the engagement beyond the end of the agreement in line with statutory periods.

§ 11 Use of data for product improvement (own purpose)

> This section governs processing that is **not** part of the processing on behalf. Insofar as riebotec uses data to improve the Software for all customers, riebotec pursues its own purpose and is itself the controller in this respect (Art. 4 (7), Art. 28 (10) GDPR). The provision clearly separates this processing from processing on behalf and ties it to an approval by the Customer that can be revoked at any time.

(1) Anonymised use without approval. riebotec may use data from the use of the Software in fully anonymised and aggregated form to operate, secure, analyse and develop the Software (e.g. usage statistics, error and performance metrics, frequency of function calls). Data is anonymised only if re-identification of data subjects or the Customer is excluded according to the state of the art with reasonable effort. Such data is not subject to the GDPR.

(2) Approval for product improvement ("Contribution to product improvement"). In addition, the Customer may permit riebotec to use the Customer's posting and document data to improve the AI assistants and document recognition for all customers, in particular for training and validating models for account, tax-rate and key-figure suggestions and for recognising document structures. The approval is **disabled by default** (opt-in) and is granted by the Customer exclusively by an administrator via the program interface under *Administration → Privacy → Contribution to product improvement*. The grant is logged with time, user and version of this provision.

(3) Scope and safeguards. For processing under para. 2 the following applies:

- Only posting lines, account assignments, tax rates, document structure features and key-figure mappings are processed. Free-text fields, names of natural persons, bank details, personnel files, vault data and employees' documents are excluded.
- Before use the data is pseudonymised: business partners are replaced by tokens, amounts are rounded or bucketed, tenant identifiers are removed. The key remains in the Customer's tenant.
- Processing takes place exclusively in the EU; no transfer to third parties outside the sub-processors named in Annex 3. Data is not passed to providers of external AI models for their own training purposes.
- Trained models contain no recoverable individual data of the Customer. riebotec verifies this before releasing any model (memorisation and extraction test) and documents the result.
- riebotec does not use the data to evaluate individual customers, business partners or persons, not for advertising purposes and not for sale to third parties.

(4) Legal basis and allocation of roles. For processing under para. 2, riebotec is the controller. The legal basis is Art. 6 (1) (f) GDPR (legitimate interest in improving the Software for the benefit of all customers) in conjunction with the Customer's approval; insofar as the Customer contributes data of natural persons, it ensures that the data subjects are informed pursuant to Art. 13/14 GDPR about the disclosure to riebotec for this purpose. riebotec provides a text module for this in the Software. The parties agree that no joint controllership under Art. 26 GDPR is established.

(5) Revocation. The Customer may revoke the approval **at any time with effect for the future** – via the same program interface (*Administration → Privacy → Contribution to product improvement → Deactivate*) or in text form to anfragen@myerp24.de. Upon revocation, riebotec ceases further use of the Customer's data for training purposes without delay, at the latest within 72 hours, and deletes unprocessed raw data from the training pools. Models already trained remain unaffected provided they contain no individual data of the Customer under para. 3; otherwise the model is withdrawn. Revocation has no effect on the usability or price of the Software.

(6) Notice in the Software. riebotec displays the status of the approval permanently in the program interface and, on each activation, points out the possibility of revocation, the scope under para. 3 and the information obligation under para. 4. Changes to this section are communicated to the Customer at least six weeks before taking effect; an approval granted lapses if the scope is extended and must be granted anew.

(7) Local learning models. Learning by the AI assistants in the Customer's browser exclusively from its own approved postings remains unaffected. These models remain in the Customer's tenant and form part of the processing on behalf.

§ 12 Liability

(1) The parties' liability is governed by Art. 82 GDPR. Internally, each party is liable for damage caused by a breach of the GDPR or this Agreement attributable to it; the parties indemnify each other accordingly.

(2) Otherwise the liability provisions of the Main Agreement apply, unless mandatory law provides otherwise.

§ 13 Final provisions

(1) Amendments and supplements to this Agreement require text form. This also applies to the waiver of this text-form requirement.

(2) Should individual provisions be invalid, the validity of the remainder of the Agreement is unaffected. The invalid provision is replaced by a provision that comes closest to the purpose of the Regulation.

(3) The law of the Federal Republic of Germany applies. Place of jurisdiction is Wuppertal, provided the Customer is a merchant, a legal entity under public law or a special fund under public law.

(4) This Agreement may be concluded electronically by acceptance in the program interface by an administrator of the Customer; riebotec provides the accepted version as a time-stamped PDF. Alternatively, the signed version applies.

Place, date · Customer (controller)	Place, date · riebotec UG (haftungsbeschränkt)

Annex 1 – Subject matter, data, data subjects

1. Nature and purpose of processing

Provision and operation of the myERP24 Software as a tenant instance: storage, processing, display, export and backup of the data entered or imported by the Customer; automated processing on behalf: document recognition (OCR, XRechnung/ZUGFeRD parsing), bank retrieval and payment matching (FinTS/import), e-invoice mailbox, posting suggestions and tax key-figure mapping by AI assistants (approval by the Customer), DATEV/GoBD export, generation of tax-form worksheets, synchronisation with Microsoft 365 (if set up by the Customer), support and error analysis.

2. Categories of personal data

Category	Examples
Business partner master data	Name, address, contact details, VAT ID, terms, bank details (IBAN), customer/supplier number
Contact persons	Name, position, phone, e-mail, communication history
Site and case data	Addresses, photos of sites, tasks, appointments, checklists, service reports
Document and posting data	Quotes, orders, invoices, supplier invoices, bank statements, postings, open items, reminders, tax key figures
Employee data of the Customer	Name, role, login, signature, working hours, mailbox assignment; personnel file (contracts, IDs, certificates – encrypted in the data vault)
Usage and log data	Logins, audit trail, IP address, timestamps, change logs
Special categories (Art. 9)	Not intended; may be contained in personnel files (e.g. disability) – only encrypted in the data vault, without evaluation by riebotec

3. Categories of data subjects

Customers, suppliers and their contact persons; prospects; employees and contractors of the Customer; users of the Software; tax advisors and other third parties involved by the Customer.

Annex 2 – Technical and organisational measures (Art. 32 GDPR)

Area	Measures
Confidentiality – physical access	Data centre in Germany with access control, video surveillance, visitor policy; riebotec office with locking system; no production data on mobile media.
Confidentiality – system access	Individual user accounts, password policy, multi-factor authentication for administrators and riebotec staff, lockout after failed attempts, session timeout, maintenance mode, registration and password workflows with administrator approval.
Confidentiality – data access	Role matrix (user, employee, coordinator, desktop user, administrator) and permission profiles, server-side check of every function; four-eyes principle on approvals; support access only after Customer approval, logged; secrets exclusively in protected configuration (configuration centre with allow-list), never in the browser.
Confidentiality – separation	Logical tenant separation at database and file level; separate environments for development, test and production; test data synthetic or anonymised.
Pseudonymisation / encryption	TLS 1.2+ for every transmission; data vault with AES-256-GCM for credentials, bank access, personnel files and certificates, key rotation, access log; encrypted backups; pseudonymisation before any use under § 11 (2).
Integrity – input/change	Immutable posting journal; finalised documents immutable, PDF archived with SHA-256; audit trail for every change with user and timestamp; versioning of templates.
Integrity – transfer	Interfaces (FinTS, Microsoft Graph, AI API, e-invoice mailbox) with minimal permissions, health checks, status per integration; transfer to the AI API only pseudonymised and without amounts/business partners (§ 11); signed support-ticket intake with duplicate protection.
Availability and resilience	Daily backup, retention 30 days rolling (max. 90 days), geographically separate copy in Germany; regular restore tests; monitoring, capacity planning, load tests; UPS, fire protection and redundant connectivity in the data centre; documented emergency and rollback plan.
Review procedures	Data protection management with annual review of the TOMs; incident-response process with 36-hour notification period; change management with review, test and backup before every release; training and commitment of staff; record of processing activities.
Control of instructions	Processing only on documented instructions; sub-processors contractually bound and regularly reviewed; deletion concept with evidence; retention-period management (anonymise instead of delete).

Annex 3 – Approved sub-processors

Company	Service	Place of processing	Safeguards
[Data centre operator, address]	Hosting, infrastructure, backup	Germany	DPA, ISO 27001 [verify]
[OCR/AI service provider, address]	Text recognition (hybrid OCR), AI API infrastructure	EU [country]	DPA, no training on customer data
[E-mail/transactional service, address]	Sending of system notifications	EU	DPA
Microsoft Ireland Operations Ltd.	Microsoft 365 (only if the Customer sets up the integration with its own tenant – then the Customer's contractual partner)	EU (EU Data Boundary)	Customer's Microsoft DPA

The current list can be viewed at any time in the Software under *Administration → Privacy → Sub-processors*. Changes are announced in accordance with § 6 (2).

Annex 4 – Text module for informing data subjects (re § 11 (4))

"To create and manage our business transactions we use the software myERP24 of riebotec UG (haftungsbeschränkt), Wuppertal, Germany, which processes your data on our behalf in Germany. Where we have approved this, riebotec uses posting and document-structure data in pseudonymised form to improve its software (Art. 6 (1) (f) GDPR). No names, contact details or bank details are used. Further information: www.myerp24.de/datenschutz."

The Customer inserts this module into its privacy information for business partners and employees as long as the approval under § 11 (2) is active.