Contrat de sous-traitance au sens de l'article 28 du RGPD

Annexe au contrat d'utilisation du logiciel myERP24

RESPONSABLE DU TRAITEMENT (« CLIENT »)

[Société, forme juridique]
[Rue, numéro]
[Code postal, ville]
représentée par : [nom, fonction]
Contact protection des données : [e-mail]

SOUS-TRAITANT (« RIEBOTEC »)

riebotec UG (haftungsbeschränkt)
Martin-Luther-Straße 15
42285 Wuppertal, Allemagne
représentée par : [gérant(e)]
Contact protection des données : anfragen@myerp24.de

Préambule

Le Client utilise l'application myERP24 (« Logiciel ») mise à disposition par riebotec en mode Software-as-a-Service sur la base des conditions générales et du contrat d'utilisation (« Contrat principal »). Dans ce cadre, riebotec traite des données à caractère personnel pour le compte du Client, notamment des données de base, de dossiers, de pièces et d'écritures du Client ainsi que des données de ses clients, fournisseurs et salariés. Le présent contrat précise les obligations des parties en matière de protection des données conformément à l'article 28, paragraphe 3, du RGPD. En cas de contradiction, il prévaut sur le Contrat principal pour les questions de protection des données.

§ 1 Objet, durée et précisions

(1) L'objet du traitement est l'exploitation du Logiciel pour le Client, y compris l'hébergement, la sauvegarde, la maintenance, le support et les fonctions décrites à l'Annexe 1 (notamment reconnaissance de pièces, récupération bancaire, boîte de factures électroniques, export DATEV, formulaires fiscaux, assistants IA).

(2) La nature et la finalité du traitement, les catégories de données à caractère personnel et les catégories de personnes concernées figurent à l'Annexe 1.

(3) La durée du traitement correspond à la durée du Contrat principal. Les obligations du § 10 (suppression et restitution) subsistent jusqu'à leur exécution complète.

(4) Le traitement a lieu exclusivement dans des États membres de l'Union européenne ou de l'Espace économique européen. L'hébergement de production est situé dans un centre de données en Allemagne (Annexe 3). Tout transfert vers un pays tiers requiert l'accord préalable du Client par écrit et le respect des articles 44 et suivants du RGPD.

§ 2 Traitement sur instruction documentée

(1) riebotec traite les données à caractère personnel exclusivement dans le cadre des accords conclus et sur instruction documentée du Client, sauf si riebotec y est tenu par le droit de l'Union ou d'un État membre ; dans ce cas, riebotec informe le Client de cette obligation juridique avant le traitement, à moins que le droit n'interdise une telle information pour des motifs importants d'intérêt public.

(2) Le Contrat principal, le présent contrat et l'utilisation des fonctions du Logiciel par le Client (y compris les paramètres définis et les traitements déclenchés par lui ou ses utilisateurs) constituent ensemble les instructions documentées. Les instructions individuelles sont transmises par écrit à anfragen@myerp24.de ou via la fonction de support du Logiciel ; les instructions orales sont confirmées sans délai par écrit.

(3) Sont habilitées à donner des instructions les personnes enregistrées comme administrateurs dans le Logiciel. Le Client notifie sans délai tout changement.

(4) Si riebotec estime qu'une instruction est contraire au droit, elle en informe immédiatement le Client et peut en suspendre l'exécution jusqu'à confirmation ou modification.

(5) Les instructions dépassant le périmètre convenu peuvent donner lieu à une rémunération distincte ; riebotec le signale avant exécution.

§ 3 Obligations et responsabilité du Client

(1) Dans le cadre du présent contrat, le Client est responsable du traitement au sens de l'article 4, point 7, du RGPD. Il est seul responsable de la licéité de la collecte, du traitement et de la transmission des données à riebotec ainsi que du respect des droits des personnes concernées, y compris des obligations d'information des articles 13 et 14 du RGPD.

(2) Le Client est responsable du respect de ses obligations commerciales et fiscales, notamment celles du § 147 AO, du § 257 HGB et des principes allemands GoBD. riebotec l'y assiste par les fonctions décrites à l'Annexe 1 (archivage probant, documentation des procédures, export Z3/GoBD, export DATEV).

(3) Le Client veille à ne saisir dans le Logiciel que des données qu'il est autorisé à traiter et à ce que les accès, rôles et droits correspondent à son concept d'habilitation.

(4) Le Client informe riebotec sans délai de toute erreur ou irrégularité constatée lors du contrôle des résultats du traitement.

§ 4 Obligations de riebotec

(1) riebotec ne traite les données que dans le cadre de la mission et des instructions du Client. Tout traitement à des fins propres est exclu, sauf disposition expresse du § 11.

(2) riebotec garantit que les personnes chargées du traitement se sont engagées à respecter la confidentialité ou sont soumises à une obligation légale appropriée de confidentialité (art. 28, par. 3, point b, RGPD) et ont été familiarisées avec les dispositions applicables avant leur prise de fonction. L'obligation de confidentialité subsiste après la fin de la mission.

(3) Lorsque la loi l'exige, riebotec a désigné un délégué à la protection des données : [nom / « non requis »]. riebotec désigne un interlocuteur responsable de la protection des données : anfragen@myerp24.de.

(4) riebotec assiste le Client, par des mesures techniques et organisationnelles appropriées, dans l'exécution de ses obligations au titre des articles 32 à 36 du RGPD (sécurité du traitement, notification des violations, analyse d'impact, consultation préalable).

(5) riebotec tient un registre de toutes les catégories d'activités de traitement conformément à l'article 30, paragraphe 2, du RGPD et en fournit au Client l'extrait le concernant sur demande.

(6) riebotec garantit que les données de production du Client sont traitées avec une stricte séparation des tenants et que tout accès du personnel riebotec aux données de production (p. ex. en support) est journalisé et n'a lieu qu'avec l'autorisation du Client via la fonction de support.

§ 5 Mesures techniques et organisationnelles

(1) riebotec met en œuvre les mesures techniques et organisationnelles décrites à l'Annexe 2 conformément à l'article 32 du RGPD. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ces mesures garantissent un niveau de sécurité adapté au risque en matière de confidentialité, d'intégrité, de disponibilité et de résilience des systèmes.

(2) Les mesures sont soumises au progrès technique. riebotec peut mettre en œuvre des mesures alternatives dès lors que le niveau de sécurité des mesures convenues n'est pas abaissé. Les modifications substantielles sont documentées et communiquées au Client sur demande.

(3) riebotec vérifie régulièrement, au moins une fois par an, l'efficacité des mesures et en documente le résultat.

§ 6 Sous-traitants ultérieurs

(1) Le Client donne à riebotec une autorisation générale de recourir à des sous-traitants ultérieurs. Ceux engagés à la date de conclusion figurent à l'Annexe 3 et sont réputés autorisés.

(2) riebotec informe le Client par écrit (e-mail aux administrateurs et avis dans le Logiciel) au moins quatre semaines avant l'ajout ou le remplacement envisagé d'un sous-traitant ultérieur. Le Client peut s'y opposer dans un délai de quatre semaines pour un motif important lié à la protection des données. En cas d'opposition sans solution amiable, chaque partie dispose d'un droit de résiliation extraordinaire du Contrat principal à la date du changement envisagé.

(3) riebotec impose contractuellement à chaque sous-traitant ultérieur les mêmes obligations de protection des données que celles du présent contrat, notamment des garanties suffisantes quant aux mesures techniques et organisationnelles appropriées (art. 28, par. 4, RGPD). Si un sous-traitant ultérieur manque à ses obligations, riebotec demeure responsable envers le Client de l'exécution de ces obligations.

(4) Ne constituent pas une sous-traitance les prestations accessoires telles que télécommunications, services postaux ou de transport, nettoyage ou maintenance sans accès aux données. riebotec y assure également une confidentialité appropriée.

§ 7 Droits des personnes concernées

(1) riebotec assiste le Client, par des mesures techniques et organisationnelles appropriées, dans son obligation de donner suite aux demandes d'exercice des droits des personnes concernées (art. 12 à 22 RGPD), notamment par des fonctions d'export, de rectification, de blocage et d'anonymisation dans le Logiciel.

(2) Si une personne concernée s'adresse directement à riebotec, celle-ci transmet la demande sans délai au Client et ne répond pas sur le fond, mais renvoie la personne vers le Client, sauf disposition légale contraire.

(3) La suppression de pièces et d'écritures soumises à conservation s'effectue conformément aux délais légaux par anonymisation des données personnelles tout en conservant le contenu comptable (« anonymiser plutôt que supprimer ») ; le Client déclenche cette fonction dans le Logiciel sous sa propre responsabilité.

§ 8 Notification des violations de données à caractère personnel

(1) riebotec notifie au Client toute violation de données à caractère personnel concernant les données du Client dans les meilleurs délais, au plus tard 36 heures après en avoir eu connaissance, aux administrateurs enregistrés et au contact protection des données du Client.

(2) Dans la mesure où elles sont déjà connues, la notification contient les informations de l'article 33, paragraphe 3, du RGPD : nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises et proposées. Les informations connues ultérieurement sont communiquées sans délai.

(3) riebotec assiste le Client dans l'exécution de ses obligations de notification et de communication envers les autorités de contrôle et les personnes concernées (art. 33, 34 RGPD). La décision de notifier appartient au Client.

(4) riebotec documente toutes les violations, leurs effets et les mesures correctives prises.

§ 9 Preuves et droits de contrôle

(1) riebotec met à disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations de l'article 28 du RGPD, notamment la version actuelle de l'Annexe 2, des rapports d'audit, des certifications ou des auto-évaluations.

(2) Le Client peut vérifier le respect du présent contrat une fois par an et, en cas de motif, de manière ponctuelle – en priorité par l'examen des documents fournis au paragraphe 1. Si ceux-ci sont insuffisants, le Client peut, après préavis raisonnable (en règle générale 14 jours), aux heures ouvrables et sans perturber l'exploitation, procéder à un contrôle sur site, lui-même ou par un tiers tenu au secret. riebotec peut refuser la désignation d'un concurrent.

(3) riebotec peut facturer, selon sa grille tarifaire en vigueur, les contrôles allant au-delà de la fourniture de documents au sens du paragraphe 1 et non motivés par des indices de manquement de riebotec.

(4) riebotec informe le Client sans délai des contrôles et mesures d'une autorité de contrôle portant sur le traitement des données du Client.

§ 10 Suppression et restitution à la fin du contrat

(1) À la fin du Contrat principal, riebotec met à disposition du Client, pendant 60 jours, l'ensemble des données stockées dans le Logiciel aux fins d'export : données de base et de dossiers en formats lisibles par machine (CSV), pièces et documents en PDF/original, écritures en export DATEV (EXTF) et export GoBD (Z3), y compris la documentation des procédures. Pendant cette période, le Logiciel est utilisable en lecture seule.

(2) À l'expiration du délai, riebotec supprime toutes les données du Client, y compris les copies, sauvegardes (après expiration de la rotation de 90 jours maximum) et journaux, sauf obligation légale de conservation incombant à riebotec. La suppression est confirmée par écrit au Client sur demande.

(3) À la demande du Client, riebotec peut fournir, contre rémunération distincte, un accès prolongé en lecture (« accès archive ») afin de soutenir ses obligations de conservation. La responsabilité de la conservation demeure celle du Client.

(4) riebotec peut conserver, au-delà de la fin du contrat et dans les délais légaux, la documentation servant à prouver un traitement conforme à la mission.

§ 11 Utilisation de données pour l'amélioration du produit (finalité propre)

> Cet article régit un traitement qui **ne relève pas** de la sous-traitance. Dans la mesure où riebotec utilise des données pour améliorer le Logiciel au bénéfice de tous les clients, elle poursuit une finalité propre et est, à ce titre, elle-même responsable du traitement (art. 4, point 7, et art. 28, par. 10, RGPD). La disposition sépare clairement ce traitement de la sous-traitance et le subordonne à une autorisation du Client révocable à tout moment.

(1) Utilisation anonymisée sans autorisation. riebotec est autorisée à utiliser des données issues de l'utilisation du Logiciel sous forme entièrement anonymisée et agrégée pour exploiter, sécuriser, analyser et développer le Logiciel (p. ex. statistiques d'utilisation, métriques d'erreurs et de performance, fréquence d'appel des fonctions). Les données ne sont anonymisées que si la ré-identification des personnes concernées ou du Client est exclue selon l'état de la technique avec des moyens raisonnables. Ces données ne relèvent pas du RGPD.

(2) Autorisation d'amélioration du produit (« Contribution à l'amélioration du produit »). Le Client peut en outre autoriser riebotec à utiliser ses données d'écritures et de pièces pour améliorer les assistants IA et la reconnaissance de pièces au bénéfice de tous les clients, notamment pour entraîner et valider des modèles de propositions de comptes, de taux de TVA et de cases fiscales ainsi que pour reconnaître des structures de pièces. L'autorisation est **désactivée par défaut** (opt-in) et n'est accordée par le Client que par un administrateur via l'interface du programme sous *Administration → Protection des données → Contribution à l'amélioration du produit*. L'octroi est journalisé avec date, utilisateur et version de la présente disposition.

(3) Périmètre et garanties. Pour le traitement du paragraphe 2 :

- Seuls sont traités les lignes d'écriture, les imputations de comptes, les taux de TVA, les caractéristiques structurelles des pièces et les affectations de cases fiscales. Les champs de texte libre, les noms de personnes physiques, les coordonnées bancaires, les dossiers du personnel, les données du coffre-fort et les documents des salariés sont exclus.
- Avant utilisation, les données sont pseudonymisées : les partenaires commerciaux sont remplacés par des jetons, les montants arrondis ou classés par tranches, les identifiants de tenant supprimés. La clé reste dans le tenant du Client.
- Le traitement a lieu exclusivement dans l'UE ; aucune transmission à des tiers autres que les sous-traitants ultérieurs de l'Annexe 3. Les données ne sont pas transmises à des fournisseurs de modèles d'IA externes à des fins d'entraînement propres.
- Les modèles entraînés ne contiennent aucune donnée individuelle récupérable du Client. riebotec le vérifie avant toute mise en production d'un modèle (test de mémorisation et d'extraction) et documente le résultat.
- riebotec n'utilise pas les données pour évaluer des clients, partenaires ou personnes individuels, ni à des fins publicitaires, ni pour les vendre à des tiers.

(4) Base juridique et répartition des rôles. Pour le traitement du paragraphe 2, riebotec est responsable du traitement. La base juridique est l'article 6, paragraphe 1, point f, du RGPD (intérêt légitime à améliorer le Logiciel au bénéfice de tous les clients) en liaison avec l'autorisation du Client ;

dans la mesure où le Client apporte des données de personnes physiques, il veille à ce que celles-ci soient informées, conformément aux articles 13/14 du RGPD, de la transmission à riebotec à cette fin. riebotec met à disposition un module de texte dans le Logiciel. Les parties conviennent qu'aucune responsabilité conjointe au sens de l'article 26 du RGPD n'est constituée.

(5) Révocation. Le Client peut révoquer l'autorisation **à tout moment avec effet pour l'avenir** – via la même interface (*Administration → Protection des données → Contribution à l'amélioration du produit → Désactiver*) ou par écrit à anfragen@myerp24.de. Dès la révocation, riebotec cesse sans délai, au plus tard sous 72 heures, toute utilisation des données du Client à des fins d'entraînement et supprime les données brutes non encore traitées des réserves d'entraînement. Les modèles déjà entraînés ne sont pas affectés dès lors qu'ils ne contiennent aucune donnée individuelle du Client au sens du paragraphe 3 ; à défaut, le modèle est retiré. La révocation n'a aucune incidence sur l'utilisabilité ou le prix du Logiciel.

(6) Mention dans le Logiciel. riebotec affiche en permanence le statut de l'autorisation dans l'interface et, à chaque activation, rappelle la possibilité de révocation, le périmètre du paragraphe 3 et l'obligation d'information du paragraphe 4. Les modifications du présent article sont communiquées au Client au moins six semaines avant leur entrée en vigueur ; une autorisation accordée devient caduque en cas d'extension du périmètre et doit être renouvelée.

(7) Modèles d'apprentissage locaux. L'apprentissage des assistants IA dans le navigateur du Client, exclusivement à partir de ses propres écritures validées, n'est pas affecté. Ces modèles restent dans le tenant du Client et relèvent de la sous-traitance.

§ 12 Responsabilité

(1) La responsabilité des parties est régie par l'article 82 du RGPD. Dans leurs rapports internes, chaque partie répond du dommage causé par une violation du RGPD ou du présent contrat qui lui est imputable ; les parties se garantissent mutuellement à ce titre.

(2) Pour le surplus, les dispositions du Contrat principal relatives à la responsabilité s'appliquent, sauf droit impératif contraire.

§ 13 Dispositions finales

(1) Toute modification ou complément du présent contrat requiert la forme écrite. Il en va de même de la renonciation à cette exigence.

(2) Si certaines dispositions étaient nulles, la validité du contrat pour le surplus n'en serait pas affectée. La disposition nulle est remplacée par une règle se rapprochant le plus de la finalité du Règlement.

(3) Le droit de la République fédérale d'Allemagne s'applique. Le tribunal compétent est celui de Wuppertal, dès lors que le Client est commerçant, personne morale de droit public ou patrimoine spécial de droit public.

(4) Le présent contrat peut être conclu par voie électronique par acceptation dans l'interface du programme par un administrateur du Client ; riebotec fournit la version acceptée en PDF horodaté. À défaut, la version signée fait foi.

Lieu, date · Client (responsable du traitement)	Lieu, date · riebotec UG (haftungsbeschränkt)

Annexe 1 – Objet, données, personnes concernées

1. Nature et finalité du traitement

Mise à disposition et exploitation du Logiciel myERP24 en tant qu'instance de tenant : stockage, traitement, affichage, export et sauvegarde des données saisies ou importées par le Client ; traitements automatisés pour le compte du Client : reconnaissance de pièces (OCR, lecture XRechnung/ZUGFeRD), récupération bancaire et lettrage (FinTS/import), boîte de factures électroniques, propositions d'écritures et d'affectation de cases fiscales par les assistants IA (validation par le Client), export DATEV/GoBD, génération de feuilles de travail pour formulaires fiscaux, synchronisation avec Microsoft 365 (si configurée par le Client), support et analyse d'erreurs.

2. Catégories de données à caractère personnel

Catégorie	Exemples
Données de base des partenaires	Nom, adresse, coordonnées, n° de TVA, conditions, coordonnées bancaires (IBAN), n° client/fournisseur
Interlocuteurs	Nom, fonction, téléphone, e-mail, historique des échanges
Données de sites et de dossiers	Adresses, photos de sites, tâches, rendez-vous, check-lists, rapports d'intervention
Pièces et écritures	Devis, commandes, factures, factures fournisseurs, relevés bancaires, écritures, postes ouverts, relances, cases fiscales
Données des salariés du Client	Nom, rôle, identifiant, signature, temps de travail, affectation de boîte mail ; dossier du personnel (contrats, pièces d'identité, certificats – chiffrés dans le coffre-fort)
Données d'utilisation et journaux	Connexions, piste d'audit, adresse IP, horodatages, journaux de modifications
Catégories particulières (art. 9)	Non prévues ; peuvent figurer dans les dossiers du personnel (p. ex. handicap) – uniquement chiffrées dans le coffre-fort, sans exploitation par riebotec

3. Catégories de personnes concernées

Clients, fournisseurs et leurs interlocuteurs ; prospects ; salariés et prestataires du Client ; utilisateurs du Logiciel ; experts-comptables et autres tiers associés par le Client.

Annexe 2 – Mesures techniques et organisationnelles (art. 32 RGPD)

Domaine	Mesures
Confidentialité – accès physique	Centre de données en Allemagne avec contrôle d'accès, vidéosurveillance, procédure visiteurs ; bureaux riebotec sécurisés ; aucune donnée de production sur supports mobiles.
Confidentialité – accès aux systèmes	Comptes individuels, politique de mots de passe, authentification multifacteur pour les administrateurs et le personnel riebotec, verrouillage après échecs, expiration de session, mode maintenance, inscription et mots de passe avec validation administrateur.
Confidentialité – accès aux données	Matrice de rôles (utilisateur, collaborateur, coordinateur, utilisateur bureau, administrateur) et profils de droits, contrôle côté serveur de chaque fonction ; principe des quatre yeux pour les validations ; accès support uniquement après autorisation du Client, journalisé ; secrets exclusivement en configuration protégée (centre de configuration avec liste blanche), jamais dans le navigateur.
Confidentialité – séparation	Séparation logique des tenants au niveau base de données et fichiers ; environnements distincts développement/test/production ; données de test synthétiques ou anonymisées.
Pseudonymisation / chiffrement	TLS 1.2+ pour toute transmission ; coffre-fort AES-256-GCM pour identifiants, accès bancaires, dossiers du personnel et certificats, rotation des clés, journal d'accès ; sauvegardes chiffrées ; pseudonymisation avant toute utilisation au titre du § 11 (2).
Intégrité – saisie/modification	Journal comptable immuable ; pièces validées immuables, PDF archivé avec SHA-256 ; piste d'audit de chaque modification avec utilisateur et horodatage ; versionnage des modèles.
Intégrité – transmission	Interfaces (FinTS, Microsoft Graph, API IA, boîte de factures électroniques) avec droits minimaux, contrôles de santé, statut par intégration ; transmission à l'API IA uniquement pseudonymisée et sans montants/partenaires (§ 11) ; réception signée des tickets de support avec protection anti-doublons.
Disponibilité et résilience	Sauvegarde quotidienne, conservation glissante 30 jours (max. 90), copie géographiquement séparée en Allemagne ; tests de restauration réguliers ; supervision, planification de capacité, tests de charge ; onduleurs, protection incendie et connectivité redondante au centre de données ; plan d'urgence et de retour arrière documenté.
Procédures de contrôle	Gestion de la protection des données avec revue annuelle des mesures ; processus de réponse aux incidents avec notification sous 36 heures ; gestion des changements avec revue, test et sauvegarde avant chaque mise en production ; formation et engagement du personnel ; registre des traitements.

Domaine	Mesures
Contrôle des instructions	Traitement uniquement sur instruction documentée ; sous-traitants ultérieurs liés contractuellement et contrôlés régulièrement ; concept de suppression avec preuve ; gestion des délais de conservation (anonymiser plutôt que supprimer).

Annexe 3 – Sous-traitants ultérieurs autorisés

Société	Prestation	Lieu du traitement	Garanties
[Exploitant du centre de données, adresse]	Hébergement, infrastructure, sauvegarde	Allemagne	Contrat de sous-traitance, ISO 27001 [à vérifier]
[Fournisseur OCR/IA, adresse]	Reconnaissance de texte (OCR hybride), infrastructure API IA	UE [pays]	Contrat de sous-traitance, pas d'entraînement sur les données clients
[Service d'e-mails transactionnels, adresse]	Envoi de notifications système	UE	Contrat de sous-traitance
Microsoft Ireland Operations Ltd.	Microsoft 365 (uniquement si le Client configure l'intégration avec son propre tenant – il est alors cocontractant du Client)	UE (EU Data Boundary)	DPA Microsoft du Client

La liste actuelle est consultable à tout moment dans le Logiciel sous *Administration → Protection des données → Sous-traitants*. Les modifications sont annoncées conformément au § 6 (2).

Annexe 4 – Module de texte pour l'information des personnes concernées (§ 11 (4))

« Pour créer et gérer nos opérations commerciales, nous utilisons le logiciel myERP24 de riebotec UG (haftungsbeschränkt), Wuppertal, Allemagne, qui traite vos données pour notre compte en Allemagne. Lorsque nous l'avons autorisé, riebotec utilise des données d'écritures et de structure de pièces sous forme pseudonymisée pour améliorer son logiciel (art. 6, par. 1, point f, RGPD). Aucun nom, aucune coordonnée ni donnée bancaire n'est utilisé. Informations complémentaires : www.myerp24.de/datenschutz. »

Le Client insère ce module dans ses informations de protection des données destinées aux partenaires et salariés tant que l'autorisation du § 11 (2) est active.