Contrato de encargo de tratamiento conforme al artículo 28 del RGPD

Anexo al contrato de uso del software myERP24

RESPONSABLE DEL TRATAMIENTO («CLIENTE»)

[Empresa, forma jurídica]
[Calle, número]
[Código postal, ciudad]
representada por: [nombre, cargo]
Contacto de privacidad: [correo]

ENCARGADO DEL TRATAMIENTO («RIEBOTEC»)

riebotec UG (haftungsbeschränkt)
Martin-Luther-Straße 15
42285 Wuppertal, Alemania
representada por: [administrador/a]
Contacto de privacidad:
anfragen@myerp24.de

Preámbulo

El Cliente utiliza la aplicación myERP24 («Software») que riebotec presta como Software-as-a-Service sobre la base de las condiciones generales y del contrato de uso («Contrato principal»). En el marco del uso, riebotec trata datos personales por cuenta del Cliente, en particular datos maestros, de expedientes, documentales y contables del Cliente, así como datos de sus clientes, proveedores y empleados. El presente contrato concreta las obligaciones de las partes en materia de protección de datos conforme al artículo 28, apartado 3, del RGPD. En caso de contradicción, prevalece sobre el Contrato principal en cuestiones de protección de datos.

§ 1 Objeto, duración y concreción

(1) El objeto del tratamiento es la operación del Software para el Cliente, incluidos alojamiento, copias de seguridad, mantenimiento, soporte y las funciones descritas en el Anexo 1 (entre otras, reconocimiento de documentos, consulta bancaria, buzón de facturas electrónicas, exportación DATEV, formularios fiscales, asistentes de IA).

(2) La naturaleza y finalidad del tratamiento, las categorías de datos personales y las categorías de interesados figuran en el Anexo 1.

(3) La duración del tratamiento coincide con la vigencia del Contrato principal. Las obligaciones del § 10 (supresión y devolución) subsisten hasta su cumplimiento íntegro.

(4) El tratamiento se realiza exclusivamente en Estados miembros de la Unión Europea o del Espacio Económico Europeo. El alojamiento productivo se encuentra en un centro de datos en Alemania (Anexo 3). Todo traslado a un tercer país requiere el consentimiento previo del Cliente por escrito y el cumplimiento de los artículos 44 y siguientes del RGPD.

§ 2 Tratamiento siguiendo instrucciones documentadas

(1) riebotec trata los datos personales exclusivamente en el marco de los acuerdos alcanzados y siguiendo instrucciones documentadas del Cliente, salvo que esté obligada a ello por el Derecho de la Unión o de un Estado miembro; en tal caso, riebotec informa al Cliente de esa exigencia legal antes del tratamiento, salvo que el Derecho lo prohíba por razones importantes de interés público.

(2) El Contrato principal, el presente contrato y el uso de las funciones del Software por el Cliente (incluidas las configuraciones realizadas y los tratamientos iniciados por él o sus usuarios) constituyen conjuntamente las instrucciones documentadas. Las instrucciones individuales se imparten por escrito a anfragen@myerp24.de o a través de la función de soporte del Software; las instrucciones verbales se confirman sin demora por escrito.

(3) Están facultadas para impartir instrucciones las personas registradas como administradores en el Software. El Cliente comunica sin demora cualquier cambio.

(4) Si riebotec considera que una instrucción infringe la ley, informa de inmediato al Cliente y puede suspender su ejecución hasta su confirmación o modificación.

(5) Las instrucciones que excedan el alcance acordado pueden ser objeto de remuneración separada; riebotec lo indica antes de ejecutarlas.

§ 3 Obligaciones y responsabilidad del Cliente

(1) En el marco de este contrato, el Cliente es el responsable del tratamiento en el sentido del artículo 4, punto 7, del RGPD. Es el único responsable de la licitud de la recogida, el tratamiento y la transmisión de los datos a riebotec, así como de la salvaguarda de los derechos de los interesados, incluidas las obligaciones de información de los artículos 13 y 14 del RGPD.

(2) El Cliente es responsable del cumplimiento de sus obligaciones mercantiles y fiscales, en particular conforme a los §§ 147 AO y 257 HGB y a los principios alemanes GoBD. riebotec le asiste mediante las funciones descritas en el Anexo 1 (archivo a prueba de auditoría, documentación de procedimientos, exportación Z3/GoBD, exportación DATEV).

(3) El Cliente garantiza que solo se introducen en el Software datos que está autorizado a tratar y que los accesos, roles y permisos se corresponden con su concepto de autorizaciones.

(4) El Cliente informa a riebotec sin demora si detecta errores o irregularidades al comprobar los resultados del tratamiento.

§ 4 Obligaciones de riebotec

(1) riebotec trata los datos únicamente en el marco del encargo y de las instrucciones del Cliente. Queda excluido el tratamiento para fines propios, salvo lo expresamente previsto en el § 11.

(2) riebotec garantiza que las personas encargadas del tratamiento se han comprometido a la confidencialidad o están sujetas a una obligación legal adecuada de confidencialidad (art. 28.3.b RGPD) y han sido instruidas en las disposiciones aplicables antes de iniciar su actividad. La obligación de confidencialidad subsiste tras el fin de la actividad.

(3) Cuando la ley lo exige, riebotec ha designado un delegado de protección de datos: [nombre / «no requerido»]. riebotec designa un interlocutor responsable de protección de datos: anfragen@myerp24.de.

(4) riebotec asiste al Cliente con medidas técnicas y organizativas apropiadas en el cumplimiento de sus obligaciones conforme a los artículos 32 a 36 del RGPD (seguridad del tratamiento, notificación de violaciones, evaluación de impacto, consulta previa).

(5) riebotec lleva un registro de todas las categorías de actividades de tratamiento conforme al artículo 30.2 del RGPD y facilita al Cliente el extracto correspondiente a petición.

(6) riebotec garantiza que los datos productivos del Cliente se tratan con estricta separación de inquilinos y que los accesos del personal de riebotec a datos productivos (p. ej., en soporte) se registran y solo tienen lugar con autorización del Cliente a través de la función de soporte.

§ 5 Medidas técnicas y organizativas

(1) riebotec aplica las medidas técnicas y organizativas descritas en el Anexo 2 conforme al artículo 32 del RGPD. Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, las medidas garantizan un nivel de seguridad adecuado al riesgo en cuanto a confidencialidad, integridad, disponibilidad y resiliencia de los sistemas.

(2) Las medidas están sujetas al progreso técnico. riebotec puede aplicar medidas alternativas siempre que no se reduzca el nivel de seguridad de las acordadas. Los cambios sustanciales se documentan y se comunican al Cliente a petición.

(3) riebotec comprueba periódicamente, al menos una vez al año, la eficacia de las medidas y documenta el resultado.

§ 6 Subencargados

(1) El Cliente otorga a riebotec una autorización general para recurrir a subencargados. Los empleados en el momento de la celebración figuran en el Anexo 3 y se consideran autorizados.

(2) riebotec informa al Cliente por escrito (correo a los administradores y aviso en el Software) con al menos cuatro semanas de antelación a la incorporación o sustitución prevista de un subencargado. El Cliente puede oponerse en el plazo de cuatro semanas por un motivo importante de protección de datos. Si se opone y no se alcanza una solución amistosa, ambas partes tienen un derecho de resolución extraordinaria del Contrato principal con efecto en la fecha del cambio previsto.

(3) riebotec impone contractualmente a cada subencargado las mismas obligaciones de protección de datos establecidas en este contrato, en particular garantías suficientes de medidas técnicas y organizativas apropiadas (art. 28.4 RGPD). Si un subencargado incumple sus obligaciones, riebotec sigue siendo responsable ante el Cliente del cumplimiento de dichas obligaciones.

(4) No constituyen subencargo los servicios accesorios como telecomunicaciones, servicios postales o de transporte, limpieza o mantenimiento sin acceso a datos. riebotec garantiza también aquí una confidencialidad adecuada.

§ 7 Derechos de los interesados

(1) riebotec asiste al Cliente con medidas técnicas y organizativas apropiadas en su obligación de responder a las solicitudes de ejercicio de los derechos de los interesados (arts. 12 a 22 RGPD), en particular mediante funciones de exportación, rectificación, bloqueo y anonimización en el Software.

(2) Si un interesado se dirige directamente a riebotec, esta remite la solicitud sin demora al Cliente y no responde sobre el fondo, sino que remite al interesado al Cliente, salvo que la ley disponga otra cosa.

(3) La supresión de documentos y asientos sujetos a conservación se realiza conforme a los plazos legales mediante la anonimización de los datos personales manteniendo el contenido contable («anonimizar en lugar de borrar»); el Cliente activa esta función en el Software bajo su propia responsabilidad.

§ 8 Notificación de violaciones de la seguridad de los datos personales

(1) riebotec notifica al Cliente toda violación de la seguridad de los datos personales que afecte a los datos del Cliente sin dilación indebida, a más tardar en 36 horas desde que tenga conocimiento, a los administradores registrados y al contacto de privacidad del Cliente.

(2) En la medida en que ya se conozcan, la notificación contiene la información del artículo 33.3 del RGPD: naturaleza de la violación, categorías y número aproximado de interesados y registros afectados, consecuencias probables, medidas adoptadas y propuestas. La información conocida posteriormente se facilita sin demora.

(3) riebotec asiste al Cliente en el cumplimiento de sus obligaciones de notificación y comunicación ante las autoridades de control y los interesados (arts. 33 y 34 RGPD). La decisión sobre las notificaciones corresponde al Cliente.

(4) riebotec documenta todas las violaciones, sus efectos y las medidas correctivas adoptadas.

§ 9 Pruebas y derechos de control

(1) riebotec pone a disposición del Cliente toda la información necesaria para demostrar el cumplimiento de las obligaciones del artículo 28 del RGPD, en particular la versión actual del Anexo 2, informes de auditoría, certificaciones o autoevaluaciones.

(2) El Cliente puede verificar el cumplimiento de este contrato una vez al año y, cuando haya motivo, de forma puntual, preferentemente mediante el examen de los documentos facilitados conforme al apartado 1. Si no bastan, el Cliente puede, previo aviso con plazo razonable (normalmente 14 días), en horario laboral y sin perturbar la operativa, realizar una inspección in situ por sí mismo o a través de un tercero obligado a confidencialidad. riebotec puede rechazar la designación de un competidor.

(3) riebotec puede facturar, según su lista de precios vigente, los controles que excedan la entrega de documentos del apartado 1 y no estén motivados por indicios de incumplimiento por su parte.

(4) riebotec informa sin demora al Cliente de los controles y medidas de una autoridad de control relativos al tratamiento de los datos del Cliente.

§ 10 Supresión y devolución al final del contrato

(1) Tras la terminación del Contrato principal, riebotec pone a disposición del Cliente durante 60 días todos los datos almacenados en el Software para su exportación: datos maestros y de expedientes en formatos legibles por máquina (CSV), documentos en PDF/original, asientos como exportación DATEV (EXTF) y exportación GoBD (Z3) incluida la documentación de procedimientos. Durante este periodo el Software puede usarse en modo de solo lectura.

(2) Transcurrido el plazo, riebotec suprime todos los datos del Cliente, incluidas copias, copias de seguridad (tras agotarse la rotación de 90 días como máximo) y registros, salvo que una obligación legal de conservación de riebotec lo impida. La supresión se confirma por escrito al Cliente a petición.

(3) A petición del Cliente, riebotec puede facilitar, contra remuneración separada, un acceso de lectura prolongado («acceso de archivo») para apoyar sus obligaciones de conservación. La responsabilidad de la conservación sigue siendo del Cliente.

(4) riebotec puede conservar, más allá del fin del contrato y dentro de los plazos legales, la documentación que acredite el tratamiento conforme al encargo.

§ 11 Uso de datos para la mejora del producto (finalidad propia)

> Este artículo regula un tratamiento que **no** forma parte del encargo de tratamiento. En la medida en que riebotec utiliza datos para mejorar el Software en beneficio de todos los clientes, persigue una finalidad propia y es, a este respecto, responsable del tratamiento (art. 4.7 y art. 28.10 RGPD). La cláusula separa claramente este tratamiento del encargo y lo condiciona a una autorización del Cliente revocable en cualquier momento.

(1) Uso anonimizado sin autorización. riebotec está facultada para utilizar datos derivados del uso del Software en forma totalmente anonimizada y agregada para operar, proteger, analizar y desarrollar el Software (p. ej., estadísticas de uso, métricas de errores y rendimiento, frecuencia de uso de funciones). Los datos solo se consideran anonimizados si la reidentificación de los interesados o del Cliente queda excluida según el estado de la técnica con un esfuerzo proporcionado. Dichos datos no están sujetos al RGPD.

(2) Autorización para la mejora del producto («Contribución a la mejora del producto»). Además, el Cliente puede permitir a riebotec utilizar sus datos contables y documentales para mejorar los asistentes de IA y el reconocimiento de documentos para todos los clientes, en particular para entrenar y validar modelos de propuestas de cuentas, tipos impositivos y casillas fiscales y para reconocer estructuras documentales. La autorización está **desactivada por defecto** (opt-in) y la concede el Cliente exclusivamente a través de un administrador en la interfaz del programa en *Administración → Protección de datos → Contribución a la mejora del producto*. La concesión se registra con fecha, usuario y versión de esta cláusula.

(3) Alcance y medidas de protección. Para el tratamiento del apartado 2 rige lo siguiente:

- Solo se tratan líneas de asiento, imputaciones contables, tipos impositivos, características estructurales de documentos y asignaciones de casillas fiscales. Quedan excluidos los campos de texto libre, nombres de personas físicas, datos bancarios, expedientes de personal, datos de la caja fuerte y documentos de los empleados.
- Antes de su uso, los datos se seudonimizan: los terceros se sustituyen por tokens, los importes se redondean o agrupan en tramos y se eliminan los identificadores de inquilino. La clave permanece en el inquilino del Cliente.
- El tratamiento se realiza exclusivamente en la UE; no hay transmisión a terceros distintos de los subencargados del Anexo 3. Los datos no se entregan a proveedores de modelos de IA externos para sus propios fines de entrenamiento.
- Los modelos entrenados no contienen datos individuales recuperables del Cliente. riebotec lo verifica antes de publicar cualquier modelo (prueba de memorización y extracción) y documenta el resultado.
- riebotec no utiliza los datos para evaluar a clientes, terceros o personas concretos, ni con fines publicitarios, ni para su venta a terceros.

(4) Base jurídica y reparto de funciones. Para el tratamiento del apartado 2, riebotec es responsable del tratamiento. La base jurídica es el artículo 6.1.f del RGPD (interés legítimo en mejorar el Software en beneficio de todos los clientes) en relación con la autorización del Cliente; en la medida en que el

Cliente aporte datos de personas físicas, garantiza que los interesados estén informados conforme a los artículos 13/14 del RGPD de la comunicación a riebotec con este fin. riebotec facilita un módulo de texto en el Software. Las partes acuerdan que no se constituye corresponsabilidad conforme al artículo 26 del RGPD.

(5) Revocación. El Cliente puede revocar la autorización **en cualquier momento con efectos para el futuro**, a través de la misma interfaz (*Administración → Protección de datos → Contribución a la mejora del producto → Desactivar*) o por escrito a anfragen@myerp24.de. Con la revocación, riebotec cesa sin demora, a más tardar en 72 horas, todo uso posterior de los datos del Cliente para fines de entrenamiento y elimina los datos brutos no procesados de las reservas de entrenamiento. Los modelos ya entrenados no se ven afectados siempre que no contengan datos individuales del Cliente conforme al apartado 3; en caso contrario, el modelo se retira. La revocación no afecta a la usabilidad ni al precio del Software.

(6) Aviso en el Software. riebotec muestra de forma permanente el estado de la autorización en la interfaz y, en cada activación, recuerda la posibilidad de revocación, el alcance del apartado 3 y la obligación de información del apartado 4. Los cambios en este artículo se comunican al Cliente con al menos seis semanas de antelación a su entrada en vigor; una autorización concedida caduca si se amplía el alcance y debe concederse de nuevo.

(7) Modelos de aprendizaje locales. No se ve afectado el aprendizaje de los asistentes de IA en el navegador del Cliente exclusivamente a partir de sus propios asientos aprobados. Estos modelos permanecen en el inquilino del Cliente y forman parte del encargo de tratamiento.

§ 12 Responsabilidad

(1) La responsabilidad de las partes se rige por el artículo 82 del RGPD. En la relación interna, cada parte responde del daño causado por una infracción del RGPD o de este contrato que le sea imputable; las partes se indemnizan mutuamente en este sentido.

(2) En lo demás rigen las disposiciones sobre responsabilidad del Contrato principal, salvo que el Derecho imperativo disponga otra cosa.

§ 13 Disposiciones finales

(1) Las modificaciones y adiciones a este contrato requieren forma escrita. Lo mismo rige para la renuncia a este requisito.

(2) Si alguna disposición fuera inválida, la validez del resto del contrato no se verá afectada. La disposición inválida se sustituye por una regla que se aproxime lo más posible a la finalidad del Reglamento.

(3) Se aplica el Derecho de la República Federal de Alemania. El fuero competente es Wuppertal, siempre que el Cliente sea comerciante, persona jurídica de Derecho público o patrimonio especial de Derecho público.

(4) Este contrato puede celebrarse electrónicamente mediante aceptación en la interfaz del programa por un administrador del Cliente; riebotec facilita la versión aceptada como PDF con sello de tiempo. Alternativamente rige la versión firmada.

Lugar, fecha · Cliente (responsable)

Lugar, fecha · riebotec UG (haftungsbeschränkt)

Anexo 1 – Objeto, datos, interesados

1. Naturaleza y finalidad del tratamiento

Puesta a disposición y operación del Software myERP24 como instancia de inquilino: almacenamiento, tratamiento, visualización, exportación y copia de seguridad de los datos introducidos o importados por el Cliente; tratamientos automatizados por cuenta del Cliente: reconocimiento de documentos (OCR, lectura XRechnung/ZUGFeRD), consulta bancaria y conciliación de pagos (FinTS/importación), buzón de facturas electrónicas, propuestas de asiento y asignación de casillas fiscales por asistentes de IA (aprobación del Cliente), exportación DATEV/GoBD, generación de hojas de trabajo de formularios fiscales, sincronización con Microsoft 365 (si el Cliente la configura), soporte y análisis de errores.

2. Categorías de datos personales

Categoría	Ejemplos
Datos maestros de terceros	Nombre, dirección, datos de contacto, NIF-IVA, condiciones, datos bancarios (IBAN), n.º de cliente/proveedor
Personas de contacto	Nombre, cargo, teléfono, correo, historial de comunicaciones
Datos de sitios y expedientes	Direcciones, fotos de sitios, tareas, citas, listas de control, partes de servicio
Datos documentales y contables	Presupuestos, pedidos, facturas, facturas de proveedores, extractos bancarios, asientos, partidas abiertas, reclamaciones, casillas fiscales
Datos de empleados del Cliente	Nombre, rol, acceso, firma, horas de trabajo, asignación de buzón; expediente de personal (contratos, documentos de identidad, certificados – cifrados en la caja fuerte)
Datos de uso y registro	Inicios de sesión, pista de auditoría, dirección IP, marcas de tiempo, registros de cambios
Categorías especiales (art. 9)	No previstas; pueden estar en expedientes de personal (p. ej., discapacidad) – solo cifradas en la caja fuerte, sin evaluación por riebotec

3. Categorías de interesados

Clientes, proveedores y sus personas de contacto; interesados comerciales; empleados y contratistas del Cliente; usuarios del Software; asesores fiscales y otros terceros implicados por el Cliente.

Anexo 2 – Medidas técnicas y organizativas (art. 32 RGPD)

Ámbito	Medidas
Confidencialidad – acceso físico	Centro de datos en Alemania con control de acceso, videovigilancia, gestión de visitantes; oficinas de riebotec con sistema de cierre; sin datos productivos en soportes móviles.
Confidencialidad – acceso a sistemas	Cuentas individuales, política de contraseñas, autenticación multifactor para administradores y personal de riebotec, bloqueo tras intentos fallidos, caducidad de sesión, modo mantenimiento, registro y contraseñas con aprobación del administrador.
Confidencialidad – acceso a datos	Matriz de roles (usuario, empleado, coordinador, usuario de escritorio, administrador) y perfiles de permisos, verificación en servidor de cada función; principio de cuatro ojos en aprobaciones; acceso de soporte solo con autorización del Cliente, registrado; secretos exclusivamente en configuración protegida (centro de configuración con lista blanca), nunca en el navegador.
Confidencialidad – separación	Separación lógica de inquilinos a nivel de base de datos y archivos; entornos separados de desarrollo, prueba y producción; datos de prueba sintéticos o anonimizados.
Seudonimización / cifrado	TLS 1.2+ en toda transmisión; caja fuerte AES-256-GCM para credenciales, accesos bancarios, expedientes de personal y certificados, rotación de claves, registro de accesos; copias de seguridad cifradas; seudonimización antes de cualquier uso conforme al § 11 (2).
Integridad – introducción/modificación	Diario contable inmutable; documentos cerrados inmutables, PDF archivado con SHA-256; pista de auditoría de cada cambio con usuario y marca de tiempo; versionado de plantillas.
Integridad – transmisión	Interfaces (FinTS, Microsoft Graph, API de IA, buzón de facturas electrónicas) con permisos mínimos, comprobaciones de estado, estado por integración; transmisión a la API de IA solo seudonimizada y sin importes/terceros (§ 11); recepción firmada de tickets de soporte con protección antiduplicados.
Disponibilidad y resiliencia	Copia de seguridad diaria, conservación rotativa 30 días (máx. 90), copia geográficamente separada en Alemania; pruebas de restauración periódicas; supervisión, planificación de capacidad, pruebas de carga; SAI, protección contra incendios y conectividad redundante en el centro de datos; plan de emergencia y reversión documentado.
Procedimientos de verificación	Gestión de protección de datos con revisión anual de las medidas; proceso de respuesta a incidentes con notificación en 36 horas; gestión de cambios con revisión, prueba y copia de seguridad antes de cada versión; formación y compromiso del personal; registro de actividades de tratamiento.
Control de instrucciones	Tratamiento solo con instrucciones documentadas; subencargados vinculados contractualmente y revisados periódicamente; concepto de supresión con acreditación; gestión de plazos de conservación (anonimizar en lugar de borrar).

Anexo 3 – Subencargados autorizados

Empresa	Servicio	Lugar del tratamiento	Garantías
[Operador del centro de datos, dirección]	Alojamiento, infraestructura, copias de seguridad	Alemania	DPA, ISO 27001 [verificar]
[Proveedor OCR/IA, dirección]	Reconocimiento de texto (OCR híbrido), infraestructura API de IA	UE [país]	DPA, sin entrenamiento con datos de clientes
[Servicio de correo transaccional, dirección]	Envío de notificaciones del sistema	UE	DPA
Microsoft Ireland Operations Ltd.	Microsoft 365 (solo si el Cliente configura la integración con su propio inquilino; en tal caso, contraparte contractual del Cliente)	UE (EU Data Boundary)	DPA de Microsoft del Cliente

La lista actual puede consultarse en cualquier momento en el Software en *Administración → Protección de datos → Subencargados*. Los cambios se anuncian conforme al § 6 (2).

Anexo 4 – Módulo de texto para informar a los interesados (§ 11 (4))

«Para crear y gestionar nuestras operaciones comerciales utilizamos el software myERP24 de riebotec UG (haftungsbeschränkt), Wuppertal, Alemania, que trata sus datos por nuestra cuenta en Alemania. Cuando lo hemos autorizado, riebotec utiliza datos contables y de estructura documental en forma seudonimizada para mejorar su software (art. 6.1.f RGPD). No se utilizan nombres, datos de contacto ni datos bancarios. Más información: www.myerp24.de/datenschutz.»

El Cliente incorpora este módulo a su información de privacidad para terceros y empleados mientras la autorización del § 11 (2) esté activa.