ข้อตกลงการประมวลผลข้อมูล ตามมาตรา 28 GDPR

ภาคผนวกของสัญญาการใช้ซอฟต์แวร์ myERP24

ผู้ควบคุมข้อมูล («ลูกค้า»)
[ชื่อบริษัท รูปแบบนิติบุคคล]
[ถนน เลขที่]
[รหัสไปรษณีย์ เมือง]
ผู้แทน: [ชื่อ ตำแหน่ง]
ผู้ติดต่อด้านความเป็นส่วนตัว: [อีเมล]

ผู้ประมวลผลข้อมูล («riebotec»)
riebotec UG (haftungsbeschränkt)
Martin-Luther-Straße 15
42285 Wuppertal ประเทศเยอรมนี
ผู้แทน: [กรรมการผู้จัดการ]
ผู้ติดต่อด้านความเป็นส่วนตัว:
anfragen@myerp24.de

อารัมภบท

ลูกค้าใช้แอปพลิเคชัน myERP24 («ซอฟต์แวร์») ที่ riebotec ให้บริการในรูปแบบ Software-as-a-Service ตามข้อกำหนดและเงื่อนไขทั่วไปและสัญญาการใช้งาน («สัญญาหลัก») ในการใช้งานนี้ riebotec ประมวลผลข้อมูลส่วนบุคคลในนามของลูกค้า โดยเฉพาะข้อมูลหลัก ข้อมูลเคส ข้อมูลเอกสารและรายการบัญชีของลูกค้า ตลอดจนข้อมูลของลูกค้า ซัพพลายเออร์ และพนักงานของลูกค้า ข้อตกลงฉบับนี้กำหนดรายละเอียดภาระหน้าที่ด้านการคุ้มครองข้อมูลของคู่สัญญาตามมาตรา 28 (3) GDPR ในกรณีที่ขัดแย้งกัน ข้อตกลงฉบับนี้มีผลเหนือสัญญาหลักในประเด็นการคุ้มครองข้อมูล

§ 1 วัตถุประสงค์ ระยะเวลา และรายละเอียด

(1) วัตถุประสงค์ของการประมวลผลคือการดำเนินงานซอฟต์แวร์สำหรับลูกค้า รวมถึงโฮสติ้ง การสำรองข้อมูล การบำรุงรักษา การสนับสนุน และฟังก์ชันที่อธิบายไว้ในภาคผนวก 1 (รวมถึงการรู้จำเอกสาร การดึงข้อมูลธนาคาร กล่องจดหมายใบแจ้งหนี้อิเล็กทรอนิกส์ การส่งออก DATEV แบบฟอร์มภาษี ผู้ช่วย AI)

(2) ลักษณะและวัตถุประสงค์ของการประมวลผล ประเภทข้อมูลส่วนบุคคล และประเภทเจ้าของข้อมูลระบุไว้ในภาคผนวก 1

(3) ระยะเวลาการประมวลผลเท่ากับระยะเวลาของสัญญาหลัก ภาระหน้าที่ตาม § 10 (การลบและการส่งคืน) คงอยู่จนกว่าจะปฏิบัติครบถ้วน

(4) การประมวลผลเกิดขึ้นเฉพาะในรัฐสมาชิกสหภาพยุโรปหรือเขตเศรษฐกิจยุโรปเท่านั้น โฮสติ้งสำหรับการใช้งานจริงตั้งอยู่ในศูนย์ข้อมูลในเยอรมนี (ภาคผนวก 3) การย้ายไปยังประเทศที่สามต้องได้รับความยินยอมล่วงหน้าเป็นลายลักษณ์อักษรจากลูกค้าและต้องปฏิบัติตามมาตรา 44 เป็นต้นไปของ GDPR

§ 2 การประมวลผลตามคำสั่งที่เป็นเอกสาร

(1) riebotec ประมวลผลข้อมูลส่วนบุคคลเฉพาะภายในกรอบข้อตกลงที่ทำไว้และตามคำสั่งที่เป็นเอกสารของลูกค้า เว้นแต่ riebotec มีหน้าที่ต้องประมวลผลตามกฎหมายของสหภาพหรือรัฐสมาชิก ในกรณีนั้น riebotec จะแจ้งข้อกำหนดทางกฎหมายดังกล่าวแก่ลูกค้าก่อนการประมวลผล เว้นแต่กฎหมายห้ามการแจ้งด้วยเหตุผลสำคัญด้านประโยชน์สาธารณะ

(2) สัญญาหลัก ข้อตกลงฉบับนี้ และการใช้ฟังก์ชันของซอฟต์แวร์โดยลูกค้า (รวมถึงการตั้งค่าและการประมวลผลที่ลูกค้าหรือผู้ใช้ของลูกค้าเป็นผู้เริ่ม) ถือเป็นคำสั่งที่เป็นเอกสารโดยรวม คำสั่งเฉพาะรายให้ส่งเป็นลายลักษณ์อักษรไปที่ anfragen@myerp24.de หรือผ่านฟังก์ชันสนับสนุนในซอฟต์แวร์ คำสั่งด้วยวาจาต้องยืนยันเป็นลายลักษณ์อักษรโดยไม่ชักช้า

(3) ผู้มีสิทธิ์ออกคำสั่งคือบุคคลที่ลงทะเบียนเป็นผู้ดูแลระบบในซอฟต์แวร์ ลูกค้าต้องแจ้งการเปลี่ยนแปลงโดยไม่ชักช้า

(4) หาก riebotec เห็นว่าคำสั่งใดขัดต่อกฎหมาย riebotec จะแจ้งลูกค้าทันทีและมีสิทธิ์ระงับการดำเนินการจนกว่าจะมีการยืนยันหรือแก้ไขคำสั่ง

(5) คำสั่งที่เกินขอบเขตบริการที่ตกลงกันอาจมีค่าตอบแทนแยกต่างหาก riebotec จะแจ้งให้ทราบก่อนดำเนินการ

§ 3 ภาระหน้าที่และความรับผิดชอบของลูกค้า

(1) ภายใต้ข้อตกลงฉบับนี้ ลูกค้าเป็นผู้ควบคุมข้อมูลตามความหมายของมาตรา 4 (7) GDPR ลูกค้ารับผิดชอบแต่เพียงผู้เดียวต่อความชอบด้วยกฎหมายของการเก็บรวบรวม การประมวลผล และการส่งข้อมูลให้ riebotec ตลอดจนการคุ้มครองสิทธิของเจ้าของข้อมูล รวมถึงหน้าที่แจ้งข้อมูลตามมาตรา 13 และ 14 GDPR

(2) ลูกค้ารับผิดชอบการปฏิบัติตามภาระหน้าที่ทางการค้าและภาษี โดยเฉพาะตาม § 147 AO, § 257 HGB และหลักการ GoBD ของเยอรมนี riebotec สนับสนุนลูกค้าผ่านฟังก์ชันที่อธิบายไว้ในภาคผนวก 1 (การจัดเก็บแบบตรวจสอบได้ เอกสารกระบวนการ การส่งออก Z3/GoBD การส่งออก DATEV)

(3) ลูกค้าต้องดูแลให้ป้อนเฉพาะข้อมูลที่ตนมีสิทธิ์ประมวลผลเข้าสู่ซอฟต์แวร์ และให้การเข้าถึง บทบาท และสิทธิ์ในซอฟต์แวร์สอดคล้องกับแนวคิดการให้สิทธิ์ของตน

(4) ลูกค้าต้องแจ้ง riebotec โดยไม่ชักช้าหากพบข้อผิดพลาดหรือความผิดปกติในการตรวจสอบผลการประมวลผล

§ 4 ภาระหน้าที่ของ riebotec

(1) riebotec ประมวลผลข้อมูลเฉพาะภายในขอบเขตของการมอบหมายและคำสั่งของลูกค้า การประมวลผลเพื่อวัตถุประสงค์ของตนเองไม่สามารถทำได้ เว้นแต่ § 11 ของข้อตกลงฉบับนี้กำหนดไว้เป็นอย่างอื่นโดยชัดแจ้ง

(2) riebotec รับรองว่าบุคคลที่เกี่ยวข้องกับการประมวลผลได้ให้คำมั่นรักษาความลับหรืออยู่ภายใต้หน้าที่รักษาความลับตามกฎหมายที่เหมาะสม (มาตรา 28 (3) (b) GDPR) และได้รับทราบบทบัญญัติด้านการคุ้มครองข้อมูลที่เกี่ยวข้องก่อนเริ่มปฏิบัติงาน หน้าที่รักษาความลับคงอยู่แม้หลังสิ้นสุดการปฏิบัติงาน

(3) หากกฎหมายกำหนด riebotec ได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล: [ชื่อ / «ไม่จำเป็น»] riebotec กำหนดผู้ติดต่อที่รับผิดชอบด้านการคุ้มครองข้อมูล: anfragen@myerp24.de

(4) riebotec สนับสนุนลูกค้าด้วยมาตรการทางเทคนิคและองค์กรที่เหมาะสมในการปฏิบัติตามภาระหน้าที่ตามมาตรา 32 ถึง 36 GDPR (ความปลอดภัยของการประมวลผล การแจ้งเหตุละเมิด การประเมินผลกระทบด้านการคุ้มครองข้อมูล การปรึกษาหารือล่วงหน้า)

(5) riebotec จัดทำบันทึกประเภทกิจกรรมการประมวลผลทั้งหมดตามมาตรา 30 (2) GDPR และจัดส่งส่วนที่เกี่ยวข้องกับลูกค้าให้เมื่อร้องขอ

(6) riebotec รับรองว่าข้อมูลจริงของลูกค้าถูกประมวลผลโดยแยกผู้เช่าอย่างเคร่งครัด และการเข้าถึงข้อมูลจริงโดยพนักงานของ riebotec (เช่น ในการสนับสนุน) จะถูกบันทึกและเกิดขึ้นเฉพาะเมื่อได้รับอนุมัติจากลูกค้าผ่านฟังก์ชันสนับสนุนเท่านั้น

§ 5 มาตรการทางเทคนิคและองค์กร

(1) riebotec ดำเนินมาตรการทางเทคนิคและองค์กรที่อธิบายไว้ในภาคผนวก 2 ตามมาตรา 32 GDPR โดยคำนึงถึงเทคโนโลยีล่าสุด ต้นทุนการดำเนินการ ตลอดจนลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผล มาตรการเหล่านี้รับประกันระดับการคุ้มครองที่เหมาะสมกับความเสี่ยงในด้านการรักษาความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน และความยืดหยุ่นของระบบ

(2) มาตรการอยู่ภายใต้ความก้าวหน้าทางเทคนิค riebotec อาจดำเนินมาตรการทางเลือกได้หากระดับความปลอดภัยของมาตรการที่ตกลงกันไม่ลดลง การเปลี่ยนแปลงที่สำคัญจะถูกบันทึกและแจ้งแก่ลูกค้าเมื่อร้องขอ

(3) riebotec ตรวจสอบประสิทธิผลของมาตรการเป็นประจำ อย่างน้อยปีละครั้ง และบันทึกผล

§ 6 ผู้ประมวลผลช่วง

(1) ลูกค้าให้อนุญาตทั่วไปแก่ riebotec ในการใช้ผู้ประมวลผลช่วง ผู้ประมวลผลช่วงที่ใช้อยู่ ณ วันทำสัญญาระบุไว้ในภาคผนวก 3 และถือว่าได้รับอนุมัติแล้ว

(2) riebotec แจ้งลูกค้าเป็นลายลักษณ์อักษร (อีเมลถึงผู้ดูแลระบบและประกาศในซอฟต์แวร์) อย่างน้อยสี่สัปดาห์ก่อนการเพิ่มหรือเปลี่ยนผู้ประมวลผลช่วงที่วางแผนไว้ ลูกค้าสามารถคัดค้านภายในสี่สัปดาห์ด้วยเหตุผลสำคัญด้านการคุ้มครองข้อมูล หากลูกค้าคัดค้านและไม่สามารถหาทางออกร่วมกันได้ คู่สัญญาทั้งสองฝ่ายมีสิทธิ์บอกเลิกสัญญาหลักเป็นกรณีพิเศษ ณ เวลาของการเปลี่ยนแปลงที่วางแผนไว้

(3) riebotec กำหนดภาระหน้าที่ด้านการคุ้มครองข้อมูลเช่นเดียวกับที่ระบุในข้อตกลงฉบับนี้แก่ผู้ประมวลผลช่วงแต่ละรายผ่านสัญญา โดยเฉพาะหลักประกันที่เพียงพอสำหรับมาตรการทางเทคนิคและองค์กรที่เหมาะสม (มาตรา 28 (4) GDPR) หากผู้ประมวลผลช่วงไม่ปฏิบัติตามภาระหน้าที่ riebotec ยังคงรับผิดต่อลูกค้าสำหรับการปฏิบัติตามภาระหน้าที่ของผู้ประมวลผลช่วงนั้น

(4) บริการเสริม เช่น โทรคมนาคม บริการไปรษณีย์/ขนส่ง การทำความสะอาด หรือการบำรุงรักษาที่ไม่มีการเข้าถึงข้อมูล ไม่ถือเป็นการประมวลผลช่วง riebotec รับรองการรักษาความลับที่เหมาะสมในกรณีเหล่านี้ด้วย

§ 7 สิทธิของเจ้าของข้อมูล

(1) riebotec สนับสนุนลูกค้าด้วยมาตรการทางเทคนิคและองค์กรที่เหมาะสมในการปฏิบัติหน้าที่ตอบสนองคำขอใช้สิทธิของเจ้าของข้อมูล (มาตรา 12 ถึง 22 GDPR) โดยเฉพาะผ่านฟังก์ชันส่งออก แก้ไข ระงับ และทำให้นิรนามในซอฟต์แวร์

(2) หากเจ้าของข้อมูลติดต่อ riebotec โดยตรง riebotec จะส่งต่อคำขอให้ลูกค้าโดยไม่ชักช้าและไม่ตอบในสาระสำคัญ แต่จะแนะนำให้เจ้าของข้อมูลติดต่อลูกค้า เว้นแต่กฎหมายกำหนดไว้เป็นอย่างอื่น

(3) การลบเอกสารและรายการบัญชีที่ต้องเก็บรักษาตามกฎหมายทำโดยการทำให้ข้อมูลส่วนบุคคลเป็นนิรนามตามระยะเวลาที่กฎหมายกำหนด โดยคงเนื้อหาที่เกี่ยวข้องกับบัญชีไว้ («ทำให้นิรนามแทนการลบ») ลูกค้าเป็นผู้เรียกใช้ฟังก์ชันนี้ในซอฟต์แวร์ด้วยความรับผิดชอบของตนเอง

§ 8 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

(1) riebotec แจ้งลูกค้าถึงเหตุละเมิดข้อมูลส่วนบุคคลที่กระทบต่อข้อมูลของลูกค้าโดยไม่ชักช้า อย่างช้าภายใน 36 ชั่วโมงหลังจากทราบเหตุ ไปยังผู้ดูแลระบบที่ลงทะเบียนและผู้ติดต่อด้านความเป็นส่วนตัวของลูกค้า

(2) เท่าที่ทราบแล้ว การแจ้งประกอบด้วยข้อมูลตามมาตรา 33 (3) GDPR: ลักษณะของการละเมิด ประเภทและจำนวนโดยประมาณของเจ้าของข้อมูลและระเบียนที่ได้รับผลกระทบ ผลที่อาจเกิดขึ้น มาตรการที่ดำเนินการและเสนอ ข้อมูลที่ทราบภายหลังจะส่งให้โดยไม่ชักช้า

(3) riebotec สนับสนุนลูกค้าในการปฏิบัติตามหน้าที่แจ้งและสื่อสารต่อหน่วยงานกำกับดูแลและเจ้าของข้อมูล (มาตรา 33, 34 GDPR) การตัดสินใจแจ้งเป็นของลูกค้า

(4) riebotec บันทึกเหตุละเมิดทั้งหมด รวมถึงผลกระทบและมาตรการแก้ไขที่ดำเนินการ

§ 9 หลักฐานและสิทธิในการตรวจสอบ

(1) riebotec จัดเตรียมข้อมูลทั้งหมดที่จำเป็นเพื่อแสดงการปฏิบัติตามภาระหน้าที่ตามมาตรา 28 GDPR แก่ลูกค้า โดยเฉพาะภาคผนวก 2 ฉบับปัจจุบัน รายงานการตรวจสอบ ใบรับรอง หรือการประเมินตนเอง

(2) ลูกค้ามีสิทธิ์ตรวจสอบการปฏิบัติตามข้อตกลงฉบับนี้ปีละครั้งและเมื่อมีเหตุ โดยหลักผ่านการตรวจสอบเอกสารที่จัดให้ตามวรรค 1 หากไม่เพียงพอ ลูกค้าอาจดำเนินการตรวจสอบ ณ สถานที่ด้วยตนเองหรือผ่านบุคคลที่สามที่ผูกพันการรักษาความลับ หลังแจ้งล่วงหน้าในระยะเวลาที่เหมาะสม (โดยทั่วไป 14 วัน) ในเวลาทำการปกติและไม่รบกวนการดำเนินงาน riebotec อาจปฏิเสธการแต่งตั้งคู่แข่ง

(3) riebotec อาจเรียกเก็บค่าใช้จ่ายตามรายการราคาปัจจุบันสำหรับการตรวจสอบที่เกินกว่าการจัดเตรียมเอกสารตามวรรค 1 และไม่ได้มีเหตุจากข้อบ่งชี้การละเมิดของ riebotec

(4) riebotec แจ้งลูกค้าโดยไม่ชักช้าถึงการตรวจสอบและมาตรการของหน่วยงานกำกับดูแลที่เกี่ยวข้องกับการประมวลผลข้อมูลของลูกค้า

§ 10 การลบและการส่งคืนหลังสิ้นสุดสัญญา

(1) หลังสิ้นสุดสัญญาหลัก riebotec จัดเตรียมข้อมูลทั้งหมดที่จัดเก็บในซอฟต์แวร์ให้ลูกค้าส่งออกเป็นเวลา 60 วัน: ข้อมูลหลักและข้อมูลเคสในรูปแบบที่เครื่องอ่านได้ (CSV) เอกสารเป็น PDF/ต้นฉบับ รายการบัญชีเป็นการส่งออก DATEV (EXTF) และการส่งออก GoBD (Z3) รวมเอกสารกระบวนการ ในช่วงเวลานี้ซอฟต์แวร์ใช้งานได้ในโหมดอ่านอย่างเดียว

(2) เมื่อพ้นกำหนด riebotec ลบข้อมูลทั้งหมดของลูกค้า รวมถึงสำเนา ข้อมูลสำรอง (หลังพ้นรอบการหมุนเวียนสำรองข้อมูลสูงสุด 90 วัน) และบันทึก เว้นแต่มีภาระหน้าที่ตามกฎหมายของ riebotec ในการเก็บรักษา การลบจะยืนยันเป็นลายลักษณ์อักษรแก่ลูกค้าเมื่อร้องขอ

(3) ตามคำขอของลูกค้า riebotec อาจจัดให้มีการเข้าถึงแบบอ่านอย่างเดียวที่ขยายเวลา («การเข้าถึงคลังเอกสาร») โดยมีค่าตอบแทนแยกต่างหากเพื่อสนับสนุนภาระหน้าที่การเก็บรักษาของลูกค้า ความรับผิดชอบในการเก็บรักษายังคงเป็นของลูกค้า

(4) riebotec อาจเก็บรักษาเอกสารที่ใช้พิสูจน์การประมวลผลที่ถูกต้องตามการมอบหมายไว้เกินกว่าสิ้นสุดสัญญาตามระยะเวลาที่กฎหมายกำหนด

§ 11 การใช้ข้อมูลเพื่อการปรับปรุงผลิตภัณฑ์ (วัตถุประสงค์ของตนเอง)

> มาตรานี้กำหนดการประมวลผลที่ **ไม่** เป็นส่วนหนึ่งของการประมวลผลในนาม ตราบเท่าที่ riebotec ใช้ข้อมูลเพื่อปรับปรุงซอฟต์แวร์สำหรับลูกค้าทุกราย riebotec ดำเนินการตามวัตถุประสงค์ของตนเองและเป็นผู้ควบคุมข้อมูลในส่วนนี้ (มาตรา 4 (7), มาตรา 28 (10) GDPR) บทบัญญัตินี้แยกการประมวลผลดังกล่าวออกจากการประมวลผลในนามอย่างชัดเจนและผูกไว้กับการอนุมัติของลูกค้าที่สามารถเพิกถอนได้ทุกเมื่อ

(1) การใช้แบบนิรนามโดยไม่ต้องอนุมัติ riebotec มีสิทธิ์ใช้ข้อมูลจากการใช้ซอฟต์แวร์ในรูปแบบนิรนามและรวมกลุ่มโดยสมบูรณ์ เพื่อดำเนินงาน รักษาความปลอดภัย วิเคราะห์ และพัฒนาซอฟต์แวร์ (เช่น สถิติการใช้งาน ตัวชี้วัดข้อผิดพลาดและประสิทธิภาพ ความถี่การเรียกใช้ฟังก์ชัน) ข้อมูลจะถือว่านิรนามก็ต่อเมื่อการระบุตัวตนเจ้าของข้อมูลหรือลูกค้าซ้ำเป็นไปไม่ได้ตามเทคโนโลยีล่าสุดด้วยความพยายามที่สมเหตุสมผล ข้อมูลดังกล่าวไม่อยู่ภายใต้ GDPR

(2) การอนุมัติเพื่อการปรับปรุงผลิตภัณฑ์ («การมีส่วนร่วมในการปรับปรุงผลิตภัณฑ์») นอกจากนี้ ลูกค้าอาจอนุญาตให้ riebotec ใช้ข้อมูลรายการบัญชีและเอกสารของลูกค้าเพื่อปรับปรุงผู้ช่วย AI และการรู้จำเอกสารสำหรับลูกค้าทุกราย โดยเฉพาะเพื่อฝึกและตรวจสอบโมเดลสำหรับข้อเสนอบัญชี อัตราภาษี และตัวเลขสำคัญตลอดจนการรู้จำโครงสร้างเอกสาร การอนุมัติ**ปิดใช้งานโดยค่าเริ่มต้น** (opt-in) และลูกค้าให้ได้เฉพาะผ่านผู้ดูแลระบบในอินเทอร์เฟซโปรแกรมที่ *การดูแลระบบ → ความเป็นส่วนตัว → การมีส่วนร่วมในการปรับปรุงผลิตภัณฑ์* การอนุมัติจะถูกบันทึกพร้อมเวลา ผู้ใช้ และเวอร์ชันของบทบัญญัตินี้

(3) ขอบเขตและมาตรการคุ้มครอง สำหรับการประมวลผลตามวรรค 2:

- ประมวลผลเฉพาะบรรทัดรายการบัญชี การกำหนดบัญชี อัตราภาษี คุณลักษณะโครงสร้างเอกสาร และการจับคู่ตัวเลขสำคัญ ฟิลด์ข้อความอิสระ ชื่อบุคคลธรรมดา ข้อมูลธนาคาร แฟ้มพนักงาน ข้อมูลตู้นิรภัย และเอกสารของพนักงานถูกยกเว้น
- ก่อนใช้งาน ข้อมูลจะถูกทำให้เป็นนามแฝง: คู่ค้าถูกแทนด้วยโทเค็น จำนวนเงินถูกปัดเศษหรือจัดกลุ่ม ตัวระบุผู้เช่าถูกลบ คีย์ยังคงอยู่ในผู้เช่าของลูกค้า
- การประมวลผลเกิดขึ้นเฉพาะใน EU ไม่มีการส่งต่อให้บุคคลที่สามนอกเหนือจากผู้ประมวลผลช่วงที่ระบุในภาคผนวก 3 ข้อมูลไม่ถูกส่งให้ผู้ให้บริการโมเดล AI ภายนอกเพื่อวัตถุประสงค์การฝึกของผู้ให้บริการเหล่านั้น
- โมเดลที่ฝึกแล้วไม่มีข้อมูลรายบุคคลของลูกค้าที่กู้คืนได้ riebotec ตรวจสอบเรื่องนี้ก่อนปล่อยโมเดลทุกครั้ง (การทดสอบการจดจำและการสกัด) และบันทึกผล
- riebotec ไม่ใช้ข้อมูลเพื่อประเมินลูกค้า คู่ค้า หรือบุคคลรายใดรายหนึ่ง ไม่ใช้เพื่อการโฆษณา และไม่ขายให้บุคคลที่สาม

(4) ฐานทางกฎหมายและการแบ่งบทบาท สำหรับการประมวลผลตามวรรค 2 riebotec เป็นผู้ควบคุมข้อมูล ฐานทางกฎหมายคือมาตรา 6 (1) (f) GDPR (ประโยชน์โดยชอบด้วยกฎหมายในการปรับปรุงซอฟต์แวร์เพื่อประโยชน์ของลูกค้าทุกราย) ประกอบกับการอนุมัติของลูกค้า ตราบเท่าที่ลูกค้านำข้อมูลของบุคคลธรรมดาเข้า

มา ลูกค้าต้องดูแลให้เจ้าของข้อมูลได้รับแจ้งตามมาตรา 13/14 GDPR เกี่ยวกับการเปิดเผยแก่ riebotec เพื่อวัตถุประสงค์นี้ riebotec จัดเตรียมข้อความสำเร็จรูปในซอฟต์แวร์ คู่สัญญาตกลงว่าไม่ก่อให้เกิดการควบคุมข้อมูลร่วมตามมาตรา 26 GDPR

(5) การเพิกถอน ลูกค้าสามารถเพิกถอนการอนุมัติ**ได้ทุกเมื่อโดยมีผลในอนาคต** – ผ่านอินเทอร์เฟซเดียวกัน (*การดูแลระบบ → ความเป็นส่วนตัว → การมีส่วนร่วมในการปรับปรุงผลิตภัณฑ์ → ปิดใช้งาน*) หรือเป็นลายลักษณ์อักษรที่ anfragen@myerp24.de เมื่อเพิกถอน riebotec จะหยุดใช้ข้อมูลของลูกค้าเพื่อการฝึกโดยไม่ชักช้า อย่างช้าภายใน 72 ชั่วโมง และลบข้อมูลดิบที่ยังไม่ได้ประมวลผลออกจากคลังข้อมูลฝึก โมเดลที่ฝึกแล้วไม่ได้รับผลกระทบหากไม่มีข้อมูลรายบุคคลของลูกค้าตามวรรค 3 มิฉะนั้นโมเดลจะถูกถอนออก การเพิกถอนไม่มีผลต่อการใช้งานหรือราคาของซอฟต์แวร์

(6) การแจ้งในซอฟต์แวร์ riebotec แสดงสถานะการอนุมัติอย่างถาวรในอินเทอร์เฟซโปรแกรม และในการเปิดใช้งานทุกครั้งจะแจ้งถึงความเป็นไปได้ในการเพิกถอน ขอบเขตตามวรรค 3 และหน้าที่แจ้งข้อมูลตามวรรค 4 การเปลี่ยนแปลงมาตรานี้จะแจ้งแก่ลูกค้าอย่างน้อยหกสัปดาห์ก่อนมีผล การอนุมัติที่ให้ไว้จะสิ้นผลเมื่อขยายขอบเขตและต้องให้ใหม่

(7) โมเดลการเรียนรู้ภายในเครื่อง การเรียนรู้ของผู้ช่วย AI ในเบราว์เซอร์ของลูกค้าจากรายการบัญชีที่อนุมัติแล้วของตนเองเท่านั้นไม่ได้รับผลกระทบ โมเดลเหล่านี้คงอยู่ในผู้เช่าของลูกค้าและเป็นส่วนหนึ่งของการประมวลผลในนาม

§ 12 ความรับผิด

(1) ความรับผิดของคู่สัญญาเป็นไปตามมาตรา 82 GDPR ในความสัมพันธ์ภายใน คู่สัญญาแต่ละฝ่ายรับผิดต่อความเสียหายที่เกิดจากการละเมิด GDPR หรือข้อตกลงฉบับนี้ที่เป็นความผิดของตน คู่สัญญาชดใช้ซึ่งกันและกันตามนั้น

(2) นอกจากนี้ให้ใช้บทบัญญัติความรับผิดของสัญญาหลัก เว้นแต่กฎหมายบังคับกำหนดไว้เป็นอย่างอื่น

§ 13 บทบัญญัติสุดท้าย

(1) การแก้ไขและเพิ่มเติมข้อตกลงฉบับนี้ต้องทำเป็นลายลักษณ์อักษร รวมถึงการยกเลิกข้อกำหนดนี้ด้วย

(2) หากบทบัญญัติใดไม่มีผล ความสมบูรณ์ของข้อตกลงส่วนที่เหลือไม่ได้รับผลกระทบ บทบัญญัติที่ไม่มีผลจะถูกแทนที่ด้วยข้อกำหนดที่ใกล้เคียงกับวัตถุประสงค์ของกฎระเบียบมากที่สุด

(3) ใช้กฎหมายของสหพันธ์สาธารณรัฐเยอรมนี ศาลที่มีเขตอำนาจคือศาลเมือง Wuppertal หากลูกค้าเป็นพ่อค้า นิติบุคคลมหาชน หรือกองทุนพิเศษมหาชน

(4) ข้อตกลงฉบับนี้สามารถทำขึ้นทางอิเล็กทรอนิกส์โดยการยอมรับในอินเทอร์เฟซโปรแกรมโดยผู้ดูแลระบบของลูกค้า riebotec จัดส่งฉบับที่ยอมรับเป็น PDF พร้อมประทับเวลา หรือให้ใช้ฉบับที่ลงนาม

สถานที่ วันที่ · ลูกค้า (ผู้ควบคุมข้อมูล)

สถานที่ วันที่ · riebotec UG (haftungsbeschränkt)

ภาคผนวก 1 – วัตถุประสงค์ ข้อมูล เจ้าของข้อมูล

1. ลักษณะและวัตถุประสงค์ของการประมวลผล

การจัดหาและดำเนินงานซอฟต์แวร์ myERP24 ในฐานะอินสแตนซ์ผู้เช่า: การจัดเก็บ ประมวลผล แสดงผล ส่งออก และสำรองข้อมูลที่ลูกค้าป้อนหรือนำเข้า; การประมวลผลอัตโนมัติในนาม: การรู้จำเอกสาร (OCR, การอ่าน XRechnung/ZUGFeRD) การดึงข้อมูลธนาคารและจับคู่การชำระเงิน (FinTS/นำเข้า) กล่องจดหมายใบแจ้งหนี้อิเล็กทรอนิกส์ ข้อเสนอรายการบัญชีและการจับคู่ตัวเลขภาษีโดยผู้ช่วย AI (ลูกค้าอนุมัติ) การส่งออก DATEV/GoBD การสร้างแผ่นงานแบบฟอร์มภาษี การซิงก์กับ Microsoft 365 (หากลูกค้าตั้งค่า) การสนับสนุนและการวิเคราะห์ข้อผิดพลาด

2. ประเภทข้อมูลส่วนบุคคล

ประเภท	ตัวอย่าง
ข้อมูลหลักคู่ค้า	ชื่อ ที่อยู่ ข้อมูลติดต่อ เลข VAT เงื่อนไข ข้อมูลธนาคาร (IBAN) เลขที่ลูกค้า/ซัพพลายเออร์
ผู้ติดต่อ	ชื่อ ตำแหน่ง โทรศัพท์ อีเมล ประวัติการสื่อสาร
ข้อมูลสถานที่และเคส	ที่อยู่ รูปภาพสถานที่ งาน นัดหมาย รายการตรวจสอบ รายงานบริการ
ข้อมูลเอกสารและรายการบัญชี	ใบเสนอราคา คำสั่งซื้อ ใบแจ้งหนี้ ใบแจ้งหนี้ซัพพลายเออร์ รายการเดินบัญชี รายการบัญชี รายการค้างชำระ หนังสือทวงถาม ตัวเลขภาษี
ข้อมูลพนักงานของลูกค้า	ชื่อ บทบาท ล็อกอิน ลายเซ็น เวลาทำงาน การกำหนดกล่องจดหมาย; แฟ้มพนักงาน (สัญญา บัตรประจำตัว ใบรับรอง – เข้ารหัสในตู้นิรภัยข้อมูล)
ข้อมูลการใช้งานและบันทึก	การเข้าสู่ระบบ บันทึกตรวจสอบ ที่อยู่ IP ประทับเวลา บันทึกการเปลี่ยนแปลง
ประเภทพิเศษ (มาตรา 9)	ไม่ได้มุ่งหมาย; อาจอยู่ในแฟ้มพนักงาน (เช่น ความพิการ) – เฉพาะแบบเข้ารหัสในตู้นิรภัย โดย riebotec ไม่ประเมิน

3. ประเภทเจ้าของข้อมูล

ลูกค้า ซัพพลายเออร์ และผู้ติดต่อของพวกเขา; ผู้สนใจ; พนักงานและผู้รับเหมาของลูกค้า; ผู้ใช้ซอฟต์แวร์; ที่ปรึกษาภาษีและบุคคลที่สามอื่นที่ลูกค้าเกี่ยวข้อง

ภาคผนวก 2 – มาตรการทางเทคนิคและองค์กร (มาตรา 32 GDPR)

ด้าน	มาตรการ
การรักษาความลับ – การเข้าถึงทางกายภาพ	ศูนย์ข้อมูลในเยอรมนีพร้อมควบคุมการเข้าออก กล้องวงจรปิด ระเบียบผู้มาเยือน; สำนักงาน riebotec มีระบบล็อก; ไม่มีข้อมูลจริงบนสื่อพกพา
การรักษาความลับ – การเข้าถึงระบบ	บัญชีผู้ใช้รายบุคคล นโยบายรหัสผ่าน การยืนยันตัวตนหลายปัจจัยสำหรับผู้ดูแลระบบและพนักงาน riebotec ล็อกหลังพยายามผิดพลาด หมดเวลาเซสชัน โหมดบำรุงรักษา เวิร์กโฟลว์ลงทะเบียนและรหัสผ่านพร้อมการอนุมัติจากผู้ดูแลระบบ
การรักษาความลับ – การเข้าถึงข้อมูล	เมทริกซ์บทบาท (ผู้ใช้ พนักงาน ผู้ประสานงาน ผู้ใช้เดสก์ท็อป ผู้ดูแลระบบ) และโปรไฟล์สิทธิ์ ตรวจสอบฝั่งเซิร์ฟเวอร์ทุกฟังก์ชัน; หลักการสี่ตาในการอนุมัติ; การเข้าถึงของฝ่ายสนับสนุนเฉพาะหลังลูกค้าอนุมัติ บันทึกไว้; ความลับอยู่ในการกำหนดค่าที่ป้องกันเท่านั้น (ศูนย์กำหนดค่าพร้อม allow-list) ไม่อยู่ในเบราว์เซอร์
การรักษาความลับ – การแยก	การแยกผู้เช่าเชิงตรรกะที่ระดับฐานข้อมูลและไฟล์; สภาพแวดล้อมแยกสำหรับพัฒนา ทดสอบ และใช้งานจริง; ข้อมูลทดสอบสังเคราะห์หรือนิรนาม
การทำให้เป็นนามแฝง / การเข้ารหัส	TLS 1.2+ สำหรับทุกการส่ง; ตู้นิรภัยข้อมูล AES-256-GCM สำหรับข้อมูลรับรองการเข้าถึงธนาคาร แฟ้มพนักงาน และใบรับรอง หมุนเวียนคีย์ บันทึกการเข้าถึง; ข้อมูลสำรองเข้ารหัส; ทำให้เป็นนามแฝงก่อนการใช้ตาม § 11 (2)
ความถูกต้องครบถ้วน – การป้อน/เปลี่ยนแปลง	สมุดรายวันบัญชีที่แก้ไขไม่ได้; เอกสารที่ยืนยันแล้วแก้ไขไม่ได้ PDF จัดเก็บพร้อม SHA-256; บันทึกตรวจสอบทุกการเปลี่ยนแปลงพร้อมผู้ใช้และประทับเวลา; การกำหนดเวอร์ชันเทมเพลต
ความถูกต้องครบถ้วน – การส่งต่อ	อินเทอร์เฟซ (FinTS, Microsoft Graph, AI API, กล่องจดหมายใบแจ้งหนี้อิเล็กทรอนิกส์) ด้วยสิทธิ์ขั้นต่ำ การตรวจสอบสถานะ สถานะต่อการเชื่อมต่อ; การส่งไปยัง AI API เฉพาะแบบนามแฝงและไม่มีจำนวนเงิน/คู่ค้า (§ 11); การรับตั๋วสนับสนุนแบบลงนามพร้อมป้องกันรายการซ้ำ
ความพร้อมใช้งานและความยืดหยุ่น	สำรองข้อมูลรายวัน เก็บแบบหมุนเวียน 30 วัน (สูงสุด 90) สำเนาแยกทางภูมิศาสตร์ในเยอรมนี; ทดสอบการกู้คืนเป็นประจำ; การตรวจสอบ การวางแผนความจุ ทดสอบโหลด; UPS ป้องกันอัคคีภัย และการเชื่อมต่อสำรองในศูนย์ข้อมูล; แผนฉุกเฉินและย้อนกลับที่บันทึกไว้
ขั้นตอนการตรวจสอบ	การจัดการคุ้มครองข้อมูลพร้อมทบทวนมาตรการประจำปี; กระบวนการตอบสนองเหตุการณ์พร้อมแจ้งภายใน 36 ชั่วโมง; การจัดการการเปลี่ยนแปลงพร้อมตรวจทาน ทดสอบ และสำรองข้อมูลก่อนทุกการปล่อย; การฝึกอบรมและคำมั่นของพนักงาน; บันทึกกิจกรรมการประมวลผล
การควบคุมคำสั่ง	ประมวลผลเฉพาะตามคำสั่งที่เป็นเอกสาร; ผู้ประมวลผลช่วงผูกพันตามสัญญาและตรวจสอบเป็นประจำ; แนวคิดการลบพร้อมหลักฐาน; การจัดการระยะเวลาเก็บรักษา (ทำให้นิรนามแทนการลบ)

ภาคผนวก 3 – ผู้ประมวลผลช่วงที่ได้รับอนุมัติ

บริษัท	บริการ	สถานที่ประมวลผล	หลักประกัน
[ผู้ให้บริการศูนย์ข้อมูล ที่อยู่]	โฮสติ้ง โครงสร้างพื้นฐาน สำรองข้อมูล	เยอรมนี	DPA, ISO 27001 [ตรวจสอบ]
[ผู้ให้บริการ OCR/AI ที่อยู่]	การรู้จำข้อความ (OCR ไฮบริด) โครงสร้างพื้นฐาน AI API	EU [ประเทศ]	DPA ไม่ฝึกด้วยข้อมูลลูกค้า
[บริการอีเมลธุรกรรม ที่อยู่]	ส่งการแจ้งเตือนระบบ	EU	DPA
Microsoft Ireland Operations Ltd.	Microsoft 365 (เฉพาะเมื่อลูกค้าตั้งค่าการเชื่อมต่อด้วยผู้เช่าของตนเอง – ในกรณีนั้นเป็นคู่สัญญาของลูกค้า)	EU (EU Data Boundary)	Microsoft DPA ของลูกค้า

รายการปัจจุบันดูได้ตลอดเวลาในซอฟต์แวร์ที่ *การดูแลระบบ → ความเป็นส่วนตัว → ผู้ประมวลผลช่วง* การเปลี่ยนแปลงจะประกาศตาม § 6 (2)

ภาคผนวก 4 – ข้อความสำเร็จรูปสำหรับแจ้งเจ้าของข้อมูล (§ 11 (4))

«ในการสร้างและจัดการธุรกรรมทางธุรกิจของเรา เราใช้ซอฟต์แวร์ myERP24 ของ riebotec UG (haftungsbeschränkt) เมือง Wuppertal ประเทศเยอรมนี ซึ่งประมวลผลข้อมูลของท่านในนามของเราในเยอรมนี ในกรณีที่เราได้อนุมัติ riebotec ใช้ข้อมูลรายการบัญชีและโครงสร้างเอกสารในรูปแบบนามแฝงเพื่อปรับปรุงซอฟต์แวร์ (มาตรา 6 (1) (f) GDPR) ไม่มีการใช้ชื่อ ข้อมูลติดต่อ หรือข้อมูลธนาคาร ข้อมูลเพิ่มเติม: www.myerp24.de/datenschutz»

ลูกค้าแทรกข้อความนี้ในประกาศความเป็นส่วนตัวของตนต่อคู่ค้าและพนักงานตราบเท่าที่การอนุมัติตาม § 11 (2) ยังมีผล