

BetriebPlus - Security & Trust

Stand: 13. August 2026 · Version: 1.0 · Status: öffentliche kundenfähige Kurzfassung

Diese Fassung ersetzt für neue Vertragsschlüsse bzw. die öffentliche Bereitstellung die Fassung vom 11.08.2026.

Anbieter: Tobias Weirich, handelnd unter „BetriebPlus“, Am Pfingstbruch 8, 34471 Volkmarsen, Deutschland · **Kontakt:** support@betriebplus.com · **Datenschutz:** datenschutz@betriebplus.com

1. Sicherheitsansatz

BetriebPlus verfolgt einen risikobasierten Sicherheitsansatz für eine mandantenfähige B2B-Webanwendung. Die Sicherheitsmaßnahmen werden an Datenarten, Rollen, technischen Pfaden und dem tatsächlichen Betriebsrisiko ausgerichtet. Diese Übersicht ist eine allgemeine öffentliche Sicherheitsinformation. Sie ist weder Zertifikat noch Garantie absoluter Sicherheit und begründet keine Beschaffenheitsvereinbarung, kein SLA und keine eigenständige Leistungspflicht. Maßgeblich für vertragliche Sicherheitsanforderungen sind der Hauptvertrag und, soweit Auftragsverarbeitung betroffen ist, der AVV einschließlich seiner TOM-Anlage. Zwingende gesetzliche Pflichten bleiben unberührt.

2. Mandantentrennung und Autorisierung

- Nutzer gehören einem Kundenbetrieb und erhalten nur rollen- und bereichsbezogene Zugriffe.
- Fachliche Zugriffsentscheidungen werden serverseitig anhand von Kundenbetrieb, Rolle, Bereich, Objekt und erforderlicher Mitgliedschaft geprüft.
- Datenbankseitige Row-Level-Security (RLS) und minimale produktive Datenbankberechtigungen bilden eine zusätzliche Schutzschicht.
- Private Direktchats sind mitgliedschaftsbasiert; ein Admin- oder Managerstatus allein vermittelt keine automatische Einsicht.

3. Authentifizierung und Zugriffsmanagement

- Geschützte Funktionen erfordern persönliche Nutzerkonten.
- Betreiber- und Servicezugriffe werden nach dem Need-to-know- und Least-Privilege-Prinzip beschränkt.
- Zugangsdaten, Secrets und technische Schlüssel werden getrennt von Quellcode und Kundeninhalten verwaltet.
- Berechtigungen werden bei Rollenwechsel oder Wegfall des Bedarfs angepasst oder entzogen.

4. Transport- und Speicherschutz

BetriebPlus stellt produktive Weboberflächen über verschlüsselte Transportverbindungen bereit. Schutzmaßnahmen für gespeicherte Daten orientieren sich an den eingesetzten Plattform- und Datenbankdiensten sowie dem jeweiligen Datenpfad. BetriebPlus verspricht keine Ende-zu-Ende-Verschlüsselung von Chats.

5. Datenminimierung und sensible Inhalte

BetriebPlus ist nicht für die Eingabe oder systematische Verarbeitung von Gesundheitsdaten oder anderen besonderen Kategorien bestimmt. Die Abwesenheitsfunktion erfasst neutral nur Person, Beginn, optionales Ende beziehungsweise "Ende noch unbekannt" und erforderliche Statusdaten. Diagnosen, Symptome, Atteste, medizinische Unterlagen und vertrauliche Personalaktendaten gehören nicht in allgemeine Freitextfelder, Chats oder Supportnachrichten. Eine permanente inhaltliche Überwachung privater Chats wird hierzu nicht eingesetzt oder zugesagt.

6. E-Rechnungen

E-Rechnungsdaten und Originalrepräsentationen werden im vorgesehenen mandantenbezogenen Daten- und Storage-Pfad verarbeitet. Zugriffe sind rollen- und mandantenbezogen geschützt. BetriebPlus ist kein revisionssicheres Langzeitarchiv und ersetzt kein gesetzlich erforderliches Buchführungs- oder Archivsystem.

7. Logging, Monitoring und Nachvollziehbarkeit

Technische Protokollierung dient Betrieb, Fehleranalyse und Sicherheit. Inhaltsdaten sollen nicht unnötig in Protokolle gelangen. Externes Verfügbarkeitsmonitoring wird auf öffentliche oder datenminimierte Endpunkte begrenzt und soll keine geschützten Kundeninhalte abrufen.

8. Backup und Wiederherstellung

Für produktive Daten bestehen Backup- und Wiederherstellungsprozesse. Datenbank, Object Storage und providerseitige Sicherungen werden dabei als unterschiedliche Schutzpfade betrachtet. Konkrete Retention-, RTO- oder RPO-Werte werden nur zugesagt, wenn sie ausdrücklich vertraglich vereinbart sind.

9. Incident Management

BetriebPlus unterhält einen Prozess zur Erkennung, Eindämmung, Untersuchung und Nachbereitung von Sicherheitsereignissen. Soweit Kundendaten betroffen sind und BetriebPlus als Auftragsverarbeiter handelt, erfolgt die Information des Kunden nach Maßgabe des AVV ohne unangemessene Verzögerung.

10. Dienstleister und Drittlandbezüge

BetriebPlus nutzt spezialisierte Infrastruktur- und Kommunikationsanbieter. Datenschutzrechtlich relevante Unterauftragsverarbeiter, Verarbeitungszwecke und Transfermechanismen werden im AVV und in der Datenschutzerklärung beschrieben. Neue oder geänderte Anbieter werden nach dem vorgesehenen Providerprozess bewertet.

11. Entwicklung und Änderungen

Sicherheitsrelevante Änderungen werden vor produktiver Nutzung geprüft. Produktive Kunden-, Beschäftigten- oder Rechnungsdaten, Datenbank-Dumps und Secrets sind kein zulässiger Inhalt des Quellcode-Repositorys. Nicht freigegebene Test- oder KI-Umgebungen dürfen nicht mit produktiven Echtdaten befüllt werden.

12. Kontakt

Sicherheitsmeldungen können an support@betriebplus.com gerichtet werden. Datenschutzanfragen sind an datenschutz@betriebplus.com zu richten. Bitte keine Passwörter, Secrets oder unnötig sensible Inhalte in die Erstmeldung aufnehmen.