Zum Hauptinhalt springen

Technische und organisatorische Maßnahmen

Anlage zur Auftragsverarbeitungsvereinbarung

Stand: 2026-10-05

Diese Anlage beschreibt die für insideBase Team und insideCRM vorgesehenen organisatorischen und technischen Schutzmaßnahmen nach Art. 32 DSGVO. Sie gilt für die Verarbeitung von Kundendaten im Rahmen der AVV. Sicherheitsrelevante Detailinformationen, die selbst ein Risiko begründen könnten, werden nur vertraulich und auf berechtigte Anfrage bereitgestellt.

1. Organisation und Berechtigungen

- Zugriffe auf produktive Kundendaten werden nach dem Need-to-know-Prinzip und anhand rollenbasierter Berechtigungen vergeben.
- Administrative Berechtigungen werden auf den erforderlichen Personenkreis beschränkt, nachvollziehbar verwaltet und regelmäßig überprüft.
- Personen mit Zugriff auf personenbezogene Daten sind auf Vertraulichkeit verpflichtet; Sicherheits- und Datenschutzvorgaben sind Bestandteil der internen Arbeitsabläufe.

2. Zugang und Authentifizierung

- Die Anwendung verwendet individuelle Nutzerkonten; gemeinsame Konten für den regulären Zugang sind nicht vorgesehen.
- Passwörter werden nicht im Klartext gespeichert. Für geeignete Konten stehen zusätzliche Schutzmechanismen wie Zwei-Faktor-Authentifizierung und Single Sign-on zur Verfügung.
- Login-, Session- und sicherheitsrelevante Ereignisse werden zur Missbrauchserkennung und Fehleranalyse protokolliert; Zugänge können bei Verdacht auf Missbrauch gesperrt oder widerrufen werden.

3. Schutz bei Übertragung, Speicherung und Verarbeitung

- Die Übertragung zwischen Browser beziehungsweise App und den Produktendpunkten erfolgt über TLS.
- Zugangsdaten, OAuth-Token und vergleichbare Geheimnisse werden in dafür vorgesehenen geschützten beziehungsweise verschlüsselten Speichermechanismen verarbeitet.
- Änderungen und Zugriffe werden, soweit es für Funktion, Sicherheit oder Nachweisführung erforderlich ist, über Protokolle und Audit-Informationen nachvollziehbar gemacht.

4. Mandantentrennung und Datenminimierung

- Kundendaten werden logisch mandantenbezogen geführt; Berechtigungsprüfungen begrenzen den Zugriff auf die jeweilige Organisation und Rolle.
- Produktfunktionen und externe Integrationen werden nur für aktivierte Zwecke bereitgestellt. Optionale Integrationen können getrennt und die zugehörigen Verknüpfungen entfernt werden.
- Entwicklungs-, Test- und Supportzugriffe auf Kundendaten werden auf das erforderliche Maß begrenzt und nach Möglichkeit von Produktivdaten getrennt.

5. Verfügbarkeit, Wiederherstellung und Löschung

- Für die Wiederherstellung werden Sicherungskopien und dokumentierte Wiederanlaufverfahren eingesetzt. Backups unterliegen einer regulären Rotation.
- Störungen, Sicherheitsereignisse und Wiederherstellungen werden nach einem risikoorientierten Verfahren bearbeitet und dokumentiert.
- Nach Vertragsende gelten die Fristen und Abläufe der Lösch- und Exportregelung; Wiederherstellungen berücksichtigen bereits vollzogene Löschungen erneut.

6. Überprüfung und Weiterentwicklung

Der Anbieter überprüft seine Schutzmaßnahmen risikoorientiert, insbesondere bei wesentlichen Änderungen an Systemen, Dienstleistern oder Verarbeitungen. Erforderliche Anpassungen werden dokumentiert. Die jeweils zum Vertragsschluss gespeicherte Fassung dieser Anlage wird zusammen mit den übrigen Vertragsunterlagen im Akzeptanznachweis festgehalten.