Zum Hauptinhalt springen

Lösch- und Exportregelung

Datenübergabe, Sperrung und Löschung nach Vertragsende

App-Konto und App-Daten löschen

Diese Anleitung gilt für die Android-Apps **insideBase** und **insideCRM** sowie die zugehörigen Webkonten.

1. Melde dich unter Kontoeinstellungen mit dem Konto an, das du löschen möchtest.
2. Öffne den Abschnitt **Konto löschen**.
3. Bestätige die Löschung mit deiner aktuellen E-Mail-Adresse und bei Passwortkonten zusätzlich mit deinem aktuellen Passwort.
4. Wähle **Konto endgültig löschen**. Die Löschung wird unmittelbar ausgeführt.

Wenn du dich nicht mehr anmelden kannst, fordere die Löschung per E-Mail an support@insideplatforms.de an. Sende die Anfrage von der im Konto hinterlegten E-Mail-Adresse und nenne die betroffene App. Wir können zur Verhinderung unberechtigter Löschungen einen Identitätsnachweis anfordern.

Gelöscht werden dein persönliches App-Konto, deine Anmeldedaten, dein persönlicher insideBase-Bereich, deine persönlichen Profileinstellungen und die direkt deinem Konto zugeordneten Daten. Bist du alleiniger Administrator eines gemeinsamen Unternehmensbereichs, musst du die Administration zuerst übertragen oder die Löschung des gesamten Mandanten durch den Inhaber beauftragen. Gemeinsame Geschäfts-, Kommunikations- und Dokumentdaten bleiben andernfalls für berechtigte Mitglieder des Unternehmensbereichs erhalten.

Produktive persönliche Kontodaten werden bei der Self-Service-Löschung unmittelbar entfernt. Daten eines vollständig zu löschenden Mandanten werden nach der unten beschriebenen Export- und Übergangsfrist innerhalb weiterer 30 Tage gelöscht oder anonymisiert. Backups werden spätestens innerhalb von 90 Tagen überschrieben. Rechnungs-, Zahlungs- und steuerrelevante Unterlagen können aufgrund gesetzlicher Pflichten regelmäßig sechs, acht oder zehn Jahre aufbewahrt werden und werden in dieser Zeit nicht für operative App-Zwecke genutzt.

1. Geltungsbereich und Export während der Vertragslaufzeit

Der Kunde kann während der Vertragslaufzeit verfügbare Self-Service-Exporte verwenden oder einen vollständigen Export beim Support anfordern. Strukturierte Daten werden grundsätzlich in einem gängigen maschinenlesbaren Format wie CSV oder JSON bereitgestellt. Dateien und Anhänge werden soweit technisch möglich in ihrem ursprünglichen Dateiformat beziehungsweise als zusammengefasstes Archiv bereitgestellt.

Der Export umfasst die dem Kunden zugeordneten Eingabedaten, erzeugten Daten und diejenigen Metadaten, die für die verständliche Zuordnung der Datensätze erforderlich sind. Ausgenommen sind Daten anderer Mandanten, interne Sicherheitsinformationen, personenbezogene Daten von Mitarbeitenden des Anbieters, Geschäftsgeheimnisse sowie Daten, deren Bereitstellung Rechte Dritter verletzen würde. Soweit die Verordnung (EU) 2023/2854 (Data Act) auf die konkrete Leistung anwendbar ist, gilt diese Regelung ergänzend als vertragliche Wechsel- und Datenübertragungsinformation.

2. Anbieterwechsel und Datenportabilität

Der Kunde kann einen Wechsel zu einem anderen Datenverarbeitungsdienst oder die Rückführung in eine eigene Infrastruktur in Textform über den Support verlangen. Die Mitteilung soll den gewünschten Wechseltermin, den Umfang, das Zielformat und – soweit einschlägig – den Zielanbieter enthalten. Der Anbieter bestätigt den Eingang und stimmt die für einen sicheren Export erforderlichen Einzelheiten mit dem Kunden ab.

Soweit der Data Act anwendbar ist, beträgt die Kündigungs- oder Ankündigungsfrist für den Wechsel höchstens zwei Monate. Nach Ablauf einer vereinbarten Ankündigungsfrist beginnt die Übergangsphase; sie beträgt grundsätzlich höchstens 30 Kalendertage. Während dieser Phase unterstützt der Anbieter die Übertragung der exportierbaren Daten und die Aufrechterhaltung der Funktionsfähigkeit, soweit dies für den Wechsel erforderlich ist.

Ist eine Übertragung innerhalb von 30 Kalendertagen technisch nicht durchführbar, informiert der Anbieter den Kunden innerhalb von 14 Arbeitstagen nach Eingang der vollständigen Wechselanfrage schriftlich über die Gründe und einen realistischen Abschlusszeitpunkt. Eine Verlängerung erfolgt nur im gesetzlich zulässigen Umfang und höchstens für den hierfür zulässigen Zeitraum. Der Kunde kann den Wechselauftrag dann fortführen oder zurücknehmen.

Für den standardisierten Export und den Wechselprozess werden keine gesonderten Wechselgebühren berechnet. Individuelle Entwicklungs-, Migrations- oder Beratungsleistungen, die über die geschuldete Datenübertragung hinausgehen, werden nur nach vorheriger ausdrücklicher Vereinbarung berechnet.

2a. Online-Register der exportierbaren Daten und Formate

Dieses Verzeichnis beschreibt die aktuell verfügbaren Datenstrukturen und Formate im Sinne des Art. 26 der Verordnung (EU) 2023/2854. Ein Export wird mandantenbezogen zusammengestellt und enthält nur Daten, zu deren Abruf der anfordernde Kunde berechtigt ist.

Datenbereich	Exportierbare Daten	Format	Bekannte Beschränkungen
CRM und Organisation	Kontakte, Leads, Kunden, Aufgaben, Tickets, Deals, Objekte, Aktivitäten, Rollen und Konfigurationen	CSV oder JSON einschließlich stabiler interner IDs und Beziehungen	Systeminterne Sicherheitsattribute, Geheimnisse und Daten anderer Mandanten sind ausgeschlossen.
Kommunikation	E-Mail-Metadaten und -Inhalte, Kalenderdaten, Chat- und Anrufmetadaten, soweit im Mandanten gespeichert	JSON; E-Mail-Inhalte zusätzlich in einem gängigen Nachrichtenformat, soweit technisch verfügbar	Providerseitig verbliebene Daten müssen gegebenenfalls beim verbundenen Anbieter exportiert werden.
Dateien und Dokumente	Hochgeladene Dateien, Bilder, Anhänge, Exposés und erzeugte Dokumente	Originalformat in einem ZIP-Archiv; begleitendes JSON-Manifest mit Pfad, Zuordnung und Prüfsumme	Verschlüsselte Passwortsafe-Inhalte werden nur in ihrer vorhandenen verschlüsselten Form exportiert.
Nachweise und Historie	Audit-, Vertragsannahme- und fachliche Verlaufsdaten im vereinbarten Umfang	CSV, JSON oder PDF, abhängig vom Nachweis	Interne Sicherheitsprotokolle und Rechte Dritter können eine Herausgabe begrenzen.

Die Exportformate verwenden UTF-8, ISO-8601-Datums- und Zeitangaben und dokumentierte Feldnamen. Ein offener, authentifizierter API-Zugriff wird bereitgestellt, soweit die jeweilige Funktion in der Leistungsbeschreibung enthalten ist. Aktuell bekannte technische Einschränkungen werden vor Beginn eines Wechselprojekts

offengelegt. Fragen zu einem konkreten Zielsystem beantwortet der Support.

2b. Infrastruktur-Rechtsordnung und Schutz vor internationalem Behördenzugriff

Die produktive Kernplattform, Datenbank und primäre Dateiverarbeitung werden in Deutschland betrieben und unterliegen deutschem Recht sowie dem Recht der Europäischen Union. Deploymentspezifischer Objektspeicher wird in der Region eu-central-1 betrieben. Optionale Integrationen können den in der Unterauftragnehmerliste bezeichneten weiteren Rechtsordnungen unterliegen.

Zum Schutz in der Union gehaltener Daten setzt der Anbieter insbesondere Zugriffsbeschränkungen, Verschlüsselung bei der Übertragung, geschützte Geheimnisverwaltung, dokumentierte Prüfung behördlicher Herausgabeersuchen, Datenminimierung und – soweit rechtlich zulässig – die Information des betroffenen Kunden ein. Herausgaben erfolgen nur auf eine rechtlich bindende Anordnung und nur im erforderlichen Umfang. Konfligierende Drittlandanfragen werden rechtlich geprüft und, soweit aussichtsreich, angefochten.

3. Abrufzeitraum, Kündigung und Übergang

Nach erfolgreicher Übergabe stehen exportierbare Daten mindestens 30 Kalendertage zum Abruf bereit, sofern kein längerer gesetzlicher Zeitraum gilt. Bis zum Ende des bezahlten Zeitraums bleibt der Mandant grundsätzlich zugänglich. Nach Vertragsende besteht eine 30-tägige Export- und Übergangsfrist. Der Zugang kann aus Sicherheits- oder Zahlungsgründen eingeschränkt werden; der Exportprozess bleibt davon unberührt, soweit keine zwingenden Gründe entgegenstehen.

4. Sperrung und produktive Löschung

Nach Ablauf des maßgeblichen Abruf- und Übergangszeitraums wird der Mandant gesperrt. Produktive Kundendaten werden innerhalb weiterer 30 Tage gelöscht oder anonymisiert. Die Löschung umfasst Datenbankeinträge, Dateien und Suchindizes, soweit diese nicht aufgrund gesetzlicher Pflichten, technischer Unvermeidbarkeit oder eines laufenden Nachweises vorübergehend weiter vorgehalten werden müssen.

5. Backups

Backups werden nicht einzeln aus dem laufenden Sicherungsbestand herausgelöscht, sondern nach der regulären Rotation überschrieben. Die maximale reguläre Aufbewahrung beträgt 90 Tage. Wiederherstellungen erfolgen nur bei berechtigtem technischem oder sicherheitsbezogenem Bedarf; nach einer Wiederherstellung wird die Löschung erneut nachvollzogen.

6. Gesetzliche Aufbewahrung

Rechnungs-, Zahlungs- und steuerrelevante Daten werden im Umfang der gesetzlichen Aufbewahrungspflichten aufbewahrt, abhängig von der jeweiligen Unterlage regelmäßig sechs, acht oder zehn Jahre. Diese Daten werden während der Aufbewahrung nicht für operative Produktzwecke genutzt, sofern dies nicht erforderlich oder zulässig ist.

7. Vorzeitige Löschung und Sonderfälle

Eine vorzeitige Löschung kann der Kunde über den Support anfordern. Gesetzliche Pflichten, offene Abrechnung, Sicherheitsuntersuchungen oder berechtigte Nachweisinteressen können einer sofortigen vollständigen Löschung entgegenstehen. Individuelle längere Export- oder Aufbewahrungsfristen müssen vor Vertragsende in Textform vereinbart werden.