Technische und organisatorische Maßnahmen (TOMs)

Anlage zur AVV von insideCRM

Version 1.3 · Stand 16.07.2026

Die nachfolgenden technischen und organisatorischen Maßnahmen sind für die produktive insideCRM-Plattform umgesetzt. Abweichende kundenspezifische Deployments werden nur berücksichtigt, wenn sie ausdrücklich vereinbart und dokumentiert wurden. Zertifizierungen oder Prüfzeichen werden nur zugesichert, wenn sie ausdrücklich genannt werden.

1. Zutrittskontrolle

Produktionssysteme und Infrastruktur werden in kontrollierten Rechenzentrumsumgebungen betrieben. Zutritte zu technischen Bereichen werden durch den jeweiligen Hostinganbieter geregelt und protokolliert. Administrative Tätigkeiten erfolgen nur durch autorisierte Personen.

2. Zugangskontrolle

Administrative Zugänge zu Produktionssystemen, Hosting, Quellcodeverwaltung, CI/CD, Datenbanken, Backup-Systemen und zentralen Drittanbieter-Accounts werden durch individuelle Konten und Mehrfaktor-Authentisierung geschützt. Gemeinsame Administratorkonten werden vermieden.

3. Zugriffskontrolle

Berechtigungen werden rollen- und mandantenbezogen vergeben. Zugriffe auf Produktionsdaten werden auf das erforderliche Maß beschränkt und bei administrativen Tätigkeiten nachvollziehbar behandelt. Der Kunde ist für die Pflege seiner Benutzer und Rollen verantwortlich.

4. Mandantentrennung

Mandanten werden logisch getrennt. Datenzugriffe werden tenantbezogen geprüft; fachliche und administrative APIs erhalten nur den für die jeweilige Funktion erforderlichen Kontext.

5. Verschlüsselung, TLS, Secrets und Tokens

Externe Verbindungen zur Plattform werden über HTTPS mit TLS 1.2 oder höher geschützt. OAuth-Tokens, API-Zugangsdaten und besonders schutzbedürftige Geheimnisse werden verschlüsselt beziehungsweise über dafür vorgesehene Secret-Mechanismen verwaltet und nicht im Quellcode gespeichert. Es wird keine pauschale Feldverschlüsselung sämtlicher CRM-Inhalte zugesichert.

Der Passwortsafe verschlüsselt Inhalte und Ordnernamen clientseitig, bevor sie gespeichert werden. Ohne Master-Passwort oder Recovery-Key können gespeicherte Safe-Inhalte aus Datenbank, Backups oder Storage nicht entschlüsselt werden. Für Betrieb und Berechtigungen notwendige technische Metadaten, etwa IDs, Zeitpunkte und Zugriffszuordnungen, bleiben sichtbar. Diese Eigenschaft gilt nicht für CRM-Datensätze, E-Mails, Chatnachrichten oder die reguläre Dateiablage. Sie schützt nicht vor kompromittierten Endgeräten, Cross-Site-Scripting oder einem manipulierten ausgelieferten Web-Frontend und ist keine Zertifizierung oder externe Sicherheitsprüfung.

6. Backup und Wiederherstellung

Produktive Datenbanken und kundenbezogene Dateien werden mindestens täglich automatisiert gesichert. Backup-Zugänge sind von normalen Anwendungszugängen getrennt. Die maximale reguläre Aufbewahrung beträgt 90 Tage. Die Wiederherstellbarkeit wird mindestens quartalsweise anhand eines dokumentierten Restore-Tests geprüft.

7. Protokollierung und Audit-Logs

Sicherheitsrelevante Anmelde-, Berechtigungs-, Administrations-, Änderungs- und Systemereignisse werden protokolliert. Passwörter, vollständige OAuth-Tokens, Client Secrets und vergleichbare Geheimnisse werden nicht protokolliert. Reguläre Sicherheits- und Anwendungslogs werden grundsätzlich bis zu 90 Tage gespeichert. Zugriffe auf Logs sind auf autorisierte Personen beschränkt.

8. Rechte- und Rollenkonzept

Administrative Berechtigungen werden bei Rollenänderungen, beim Ausscheiden einer berechtigten Person und zusätzlich mindestens quartalsweise überprüft. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.

9. Entwicklungs-, Test- und Produktionsumgebungen

Entwicklung, Test und Produktion werden organisatorisch und technisch getrennt betrieben. Produktivdaten werden nicht ohne Zweck und Schutzmaßnahmen in Entwicklungs- oder Testumgebungen verwendet. Änderungen werden vor dem Produktiveinsatz geprüft.

10. Patch-, Update- und Change-Prozess

Sicherheitsupdates und Abhängigkeiten werden risikobasiert bewertet und eingespielt. Änderungen werden versioniert, geprüft und nach Möglichkeit reproduzierbar ausgerollt. Kritische Fehlerbehebungen können außerhalb regulärer Wartungsfenster erforderlich sein.

11. Incident-Response

Sicherheits- und Verfügbarkeitsvorfälle werden aufgenommen, bewertet, eingedämmt und nachbereitet. Betroffene Kunden werden informiert, wenn eine meldepflichtige oder für ihre Daten relevante Verletzung bekannt wird. Wiederkehrende Ursachen werden soweit angemessen durch Maßnahmen reduziert.

12. Löschkonzept

Löschungen berücksichtigen Vertragsstatus, Exportfrist, operative Daten, Backups und gesetzliche Aufbewahrungspflichten. Die konkreten Fristen sind in der Lösch- und Exportregelung beschrieben.

13. Dienstleisterkontrolle

Unterauftragnehmer werden vor Einsatz nach Zweck, Vertrag, Sicherheitsinformationen und Datenschutzanforderungen bewertet. Änderungen werden in der Unterauftragnehmerliste dokumentiert und nach dem AVV-Prozess angekündigt.

14. Regelmäßige Überprüfung

Die Maßnahmen werden regelmäßig und anlassbezogen überprüft, insbesondere bei wesentlichen Änderungen der Architektur, des Deployments, der Bedrohungslage oder der rechtlichen Anforderungen. Die Maßnahmen ersetzen keine individuelle Sicherheitsprüfung des Kunden.