Zum Hauptinhalt springen

Datenschutzerklärung

Diese Datenschutzerklärung gilt für die öffentliche Website unter **https://insidecrm.de** sowie für alle damit verbundenen Produkt-, Login-, Consent-, Support-, Mobile-App- und API-Angebote, auf denen auf diese Datenschutzerklärung verwiesen wird.

Sie beschreibt, welche personenbezogenen Daten wir als Verantwortlicher für Website, Registrierung, Billing, Support und Integrationen verarbeiten und wie wir mit Daten umgehen, die im Rahmen der insideCRM-Plattform im Auftrag unserer Kunden verarbeitet werden.

---

1. Verantwortlicher

Verantwortlicher im Sinne der DSGVO für die in dieser Erklärung beschriebenen Verarbeitungen ist:

Leonhard Frühwald GmbH

Kellerweg 15

91459 Markt Erlbach

DE

Niederlassung

Wilhelmstraße 2

91413 Neustadt an der Aisch

Telefon: 09106 9640985-0

E-Mail: info@insidecrm.de

Weitere gesetzliche Pflichtangaben stellen wir im Impressum bereit.

2. Rollenverständnis: Verantwortlicher und Auftragsverarbeiter

Für den Betrieb der Homepage, Kontaktanfragen, Testzugänge, Nutzerkonten, Verträge, Rechnungen, Zahlungen, technische Sicherheit, Produktkommunikation und die Verwaltung von Integrationen handeln wir grundsätzlich als **Verantwortlicher**.

Soweit unsere Kunden in insideCRM eigene Leads, Kontakte, Deals, Tickets, Dokumente, Kommunikationsinhalte, Kalenderdaten oder andere Geschäftsdaten verwalten, verarbeiten wir diese Daten in der Regel als **Auftragsverarbeiter** nach Weisung des jeweiligen Kunden. In diesem Fall richtet sich die datenschutzrechtliche Zulässigkeit der fachlichen Verarbeitung primär nach dem Kundenverhältnis und den dort vereinbarten Verträgen, insbesondere einer AVV.

3. Kategorien personenbezogener Daten

- **Website- und Kontaktdaten**, etwa Name, E-Mail-Adresse, Team/Bereich, Nachrichteninhalt, IP-Adresse, Zeitstempel und technische Metadaten.
- **Account- und Registrierungsdaten**, etwa Anmeldename, E-Mail-Adresse, Rollen, Login-Status, Zwei-Faktor-Status und Verifikationsdaten.
- **Vertrags- und Billing-Daten**, etwa Firma, Rechnungsadresse, USt-IdNr., Vertragsstatus, Lizenzdaten, Zahlungsstatus und abrechnungsrelevante Metadaten.
- **Integrationsdaten**, etwa OAuth-Kennungen, Scopes, Refresh- und Access-Token, Postfach- oder Kalenderreferenzen sowie Synchronisationsmetadaten.
- **Plattform- und CRM-Inhaltsdaten**, soweit Kunden diese in insideCRM verarbeiten, etwa Kontakt-, Deal-, Ticket-, Notiz-, Datei-, E-Mail-, Kalender- oder Messaging-Inhalte.
- **Audio-, Sprach- und KI-bezogene Daten**, wenn Nutzer entsprechende Funktionen aktiv verwenden, etwa Audioanhänge, Transkripte, Prompts, Zusammenfassungen oder KI-Ausgaben.
- **Sicherheits- und Protokolldaten**, etwa IP-Adressen, Geräteinformationen, Session-IDs, Fehlerlogs, Audit-Logs und Missbrauchsindikatoren.

4. Zwecke und Rechtsgrundlagen

- **Bereitstellung der Website:** Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse besteht im sicheren und stabilen Betrieb unseres Online-Angebots.
- **Kontakt- und Demoanfragen:** Art. 6 Abs. 1 lit. b DSGVO bei Vertragsanbahnung oder bestehenden Verträgen, ansonsten Art. 6 Abs. 1 lit. f DSGVO.
- **Registrierung und Vertragskonten:** Art. 6 Abs. 1 lit. b DSGVO, soweit die betroffene Person selbst Vertragspartner ist. Bei Mitarbeitern und Nutzern eines Unternehmenskunden erfolgt die Verarbeitung insbesondere auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO sowie im Rahmen der Auftragsverarbeitung nach Weisung des Kunden.
- **Vertragsmanagement, Abrechnung und Rechnungsstellung:** Art. 6 Abs. 1 lit. b und lit. c DSGVO.
- **IT-Sicherheit, Missbrauchsprävention, Protokollierung und Fehleranalyse:** Art. 6 Abs. 1 lit. f DSGVO.
- **Vom Kunden aktivierte Integrationen:** zur Vertragsdurchführung beziehungsweise im Rahmen der dokumentierten Weisung des Kunden. Eine Einwilligung wird nur verwendet, wenn sie für die konkrete Funktion tatsächlich erforderlich ist.
- **KI-, Voice- und Transkriptionsfunktionen:** zur Bereitstellung der vom Kunden aktivierten Funktion beziehungsweise im Rahmen seiner dokumentierten Weisung. Erforderliche Einwilligungen der Gesprächsteilnehmer muss der Kunde vor Beginn der Verarbeitung einholen.

Unser berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO liegt insbesondere in der sicheren, stabilen und missbrauchsfreien Bereitstellung der Website und Plattform, der Abwehr automatisierter Angriffe sowie der Fehleranalyse. Angaben für Registrierung, Vertragsverwaltung und Abrechnung sind für die Anbahnung oder Durchführung des Vertrags erforderlich. Ohne diese Angaben können wir kein Nutzerkonto, keinen Testmandanten oder kostenpflichtigen Vertrag bereitstellen; freiwillige Angaben sind entsprechend gekennzeichnet.

5. Kontaktformular und Website-Kommunikation

Wenn du uns über das Kontaktformular kontaktierst, verarbeiten wir deinen Namen, deine E-Mail-Adresse, dein Team beziehungsweise deinen Bereich, deine Nachricht

und technische Verbindungsdaten, um deine Anfrage zu prüfen, zu beantworten und Missbrauch zu verhindern. Formulare werden durch lokale Plausibilitätsprüfungen und serverseitige Anfragelimits geschützt; dafür laden wir keinen externen Sicherheitsdienst.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, wenn sich deine Anfrage auf eine Vertragsanbahnung oder einen bestehenden Vertrag bezieht, ansonsten Art. 6 Abs. 1 lit. f DSGVO. Kontaktanfragen speichern wir grundsätzlich bis zur abschließenden Bearbeitung und danach noch bis zu **12 Monate**, sofern keine gesetzliche Aufbewahrungspflicht oder ein Anschlussvertrag eine längere Speicherung erfordert.

6. Login, SSO und OAuth-Integrationen

Wenn du Single-Sign-on oder OAuth-Integrationen mit Google oder Microsoft nutzt, verarbeiten wir die für Anmeldung, Autorisierung, Token-Verwaltung und Synchronisation erforderlichen Daten. Dazu können insbesondere Benutzerkennung, E-Mail-Adresse, angeforderte Berechtigungen, Tenant- oder Domainbezug, Refresh- und Access-Token sowie technische Ereignis- und Fehlerdaten gehören.

Wir verwenden diese Daten ausschließlich, um die von dir oder deinem Unternehmen aktivierte Funktion bereitzustellen, Zugriffe zu authentifizieren, Postfächer oder Kalender zu verbinden, Synchronisationen auszuführen und sicherheitsrelevante Ereignisse nachzuvollziehen. Wir nutzen Google-Workspace- oder Microsoft-365-Daten nicht für Werbung, verkaufen diese Daten nicht und verwenden sie nicht zum Training allgemeiner KI-Modelle, soweit wir solche Daten aus diesen Diensten erhalten.

Schutz öffentlicher Formulare mit Google reCAPTCHA

Für Kontaktanfragen, E-Mail-Registrierungen und Passwort-Reset-Anfragen verwenden wir Google reCAPTCHA Enterprise. Die Prüfung startet beim Absenden des Formulars und bewertet technische Signale der Browserinteraktion, ohne eine Checkbox oder Bilderaufgabe anzuzeigen. Unser Server übermittelt das erzeugte Prüfungstoken, den Aktionsnamen und die Browserkennung an Google. Google bewertet die Gültigkeit des Tokens und das Missbrauchsrisiko. Formularinhalte und Passwörter werden von unserer reCAPTCHA-Einbindung nicht an die Bewertungs-API übertragen. Weitere Informationen findest du in der Datenschutzerklärung von Google.

7. Google User Data, Google- und Microsoft-Daten

Bei aktivierter Integration können wir je nach Funktionsumfang Profildaten, E-Mail-Metadaten, Inhalte aus verbundenen Postfächern, Kalenderinformationen oder zugehörige Synchronisationsdaten verarbeiten. Welche Daten konkret verarbeitet werden, hängt von den im Consent freigegebenen Berechtigungen und der aktivierten Funktion ab.

insideCRM nutzt Google User Data ausschließlich, um vom Nutzer autorisierte Funktionen bereitzustellen: Google Login, Gmail-Mailbox-Verbindung, E-Mail-Synchronisation, E-Mail-Anzeige, Label-/Ordnerabbildung, E-Mail-Versand und Mailbox-Aktualisierungen.

insideCRM verkauft Google User Data nicht, nutzt diese Daten nicht für Werbung und gibt sie nicht an Dritte weiter, außer soweit dies zur Bereitstellung der insideCRM-Funktionen, zur Sicherheit, zur Fehlerbehebung oder aufgrund gesetzlicher Pflichten erforderlich ist.

Google User Data wird nur solange gespeichert, wie dies für die autorisierten Funktionen, Synchronisationen, Sicherheitsprüfungen, Fehlerbehebung oder gesetzliche Pflichten erforderlich ist. Nicht mehr benötigte OAuth-Tokens, Verknüpfungen und Synchronisationsdaten löschen oder anonymisieren wir nach Deaktivierung der Integration grundsätzlich innerhalb von **30 Tagen**, sofern keine gesetzlichen Pflichten oder laufenden Sicherheitsuntersuchungen entgegenstehen.

Microsoft-Daten verwenden wir ausschließlich zur Bereitstellung der angeforderten Funktionen innerhalb von insideCRM, etwa für Anmeldung, Postfachanbindung, Terminabgleich, Kommunikation, Suchfunktionen, Automationen oder nutzerseitig ausgelöste CRM-Prozesse. Eine Weitergabe erfolgt nur an technisch erforderliche Dienstleister oder, wenn dies rechtlich geboten ist.

Die Nutzung und Übertragung von Informationen, die insideCRM von Google APIs erhält, erfolgt gemäß der Google API Services User Data Policy einschließlich der Limited Use Requirements.

Mitarbeiter oder beauftragte Personen erhalten keinen inhaltlichen Zugriff auf Google User Data, außer wenn der betroffene Nutzer den Zugriff für einen konkreten Supportfall ausdrücklich freigegeben hat, der Zugriff für Sicherheits- oder Missbrauchsuntersuchungen erforderlich ist oder eine gesetzliche Verpflichtung besteht.

8. Telefonie und Voice-Funktionen

Bei der Nutzung von Voice-Funktionen verarbeitet insideCRM abhängig von der aktivierten Funktion Benutzerkennungen, Telefonnummern, Geräte- und Push-Token, Anrufzeitpunkte, Verbindungsstatus, Gesprächsdauer, technische Ereignisdaten und Zuordnungen zu CRM-Datensätzen. Für die technische Bereitstellung kann Twilio eingesetzt werden. Der jeweilige Nutzer muss seine ausgehende Rufnummer vor der ersten externen Verbindung verifizieren. Interne Gespräche werden unabhängig davon über die interne Voice-Infrastruktur bereitgestellt.

Gesprächsinhalte werden nicht automatisch aufgezeichnet. Soweit eine Aufzeichnungs- oder Transkriptionsfunktion angeboten und vom Kunden aktiviert wird, darf sie erst verwendet werden, nachdem alle betroffenen Gesprächsteilnehmer rechtmäßig informiert wurden und erforderliche Einwilligungen vorliegen. Die Aktivierung und der Aufzeichnungsstatus werden in der Anwendung sichtbar gemacht.

9. KI-Funktionen und Audio-Transkription

Wenn KI- oder Transkriptionsfunktionen in insideCRM aktiviert sind, können Eingaben, Dateien, Audioanhänge, Transkripte, Systemhinweise, generierte Inhalte und technische Nutzungsmetadaten verarbeitet werden, soweit dies für die angeforderte Funktion erforderlich ist.

Wir setzen solche Verarbeitungen ausschließlich ein, um die vom Nutzer ausgelöste Funktion auszuführen, etwa Zusammenfassungen, Textentwürfe, Extraktionen oder Transkripte. Inhalte aus Google- oder Microsoft-Workspace-Integrationen werden dabei nicht zum Training allgemeiner KI-Modelle verwendet. Audio-Dateien und Transkripte löschen wir grundsätzlich mit dem zugrunde liegenden Datensatz oder nach manueller Entfernung; technisch bedingte Zwischenstände werden regelmäßig innerhalb von **30 Tagen** bereinigt, sofern keine längere Speicherung durch den Kunden veranlasst ist.

KI-generierte Ergebnisse werden innerhalb der Anwendung als solche erkennbar gemacht. Ergebnisse können unvollständig oder fehlerhaft sein und müssen vor einer geschäftlichen, rechtlichen oder finanziellen Verwendung durch einen Menschen geprüft werden. insideCRM trifft auf Grundlage der KI-Ausgabe keine rechtlich verbindlichen Entscheidungen über betroffene Personen.

10. Empfänger, Dienstleister und Subprocessor-Kategorien

Wir geben personenbezogene Daten nur weiter, wenn dies zur Vertragserfüllung, zur Bereitstellung aktivierter Funktionen, zur Erfüllung rechtlicher Pflichten oder auf Basis berechtigter Interessen erforderlich ist. Dabei können insbesondere folgende Empfänger oder Kategorien eingebunden sein:

- **Hosting und Infrastruktur**, etwa Server-, Datenbank-, Storage-, Backup- und Netzwerkdienstleister.
- **Zahlungsdienstleister**, insbesondere Stripe, für Zahlungsabwicklung, Betrugsprävention und Abrechnung.
- **Kommunikations- und Produktivitätsdienste**, etwa Microsoft 365, Microsoft Graph, Google Workspace oder Teams, sofern Kunden diese Funktionen aktiv verbinden.
- **KI- und Transkriptionsdienste**, etwa OpenAI, wenn entsprechende Funktionen aktiv eingesetzt werden.
- **E-Mail- und Support-Dienste** für Systemnachrichten, Rechnungen und Supportkommunikation.

Eine aktuelle Übersicht der Standard- und optionalen Dienstleister, ihrer Rollen und Transfermechanismen steht in unserer Unterauftragnehmerliste. Soweit Dienstleister als Auftragsverarbeiter eingesetzt werden, schließen wir die erforderlichen Verträge ab.

11. Drittlandtransfers

Soweit wir Dienstleister oder Integrationen mit Sitz außerhalb der EU beziehungsweise des EWR einsetzen oder ein Zugriff aus Drittländern nicht ausgeschlossen werden kann, achten wir auf geeignete Garantien nach Art. 44 ff. DSGVO. Dazu können insbesondere Angemessenheitsbeschlüsse, Standardvertragsklauseln, ergänzende technische und organisatorische Maßnahmen oder andere gesetzlich anerkannte Transfermechanismen gehören. Informationen über die jeweils einschlägige Garantie oder eine Kopie der maßgeblichen Garantien kannst du unter info@insidecrm.de anfordern, soweit die Herausgabe rechtlich zulässig ist.

12. Cookies, Sessions und technische Sicherheit

Wir verwenden auf den öffentlichen Seiten und in der Anwendung technisch erforderliche Cookies, Session-Mechanismen und Sicherheitsfunktionen, insbesondere für Login, Session-Handling, CSRF-Schutz, Lastverteilung, Spracheinstellungen und Missbrauchsprävention. Ohne diese Mechanismen ist ein sicherer Betrieb nicht möglich.

Zum Schutz personenbezogener Daten setzen wir abhängig von der jeweiligen Funktion insbesondere Transportverschlüsselung, rollenbasierte Zugriffe, Protokollierung sicherheitsrelevanter Ereignisse, Zugriffsbeschränkungen, Backup- und Wiederherstellungsverfahren sowie Maßnahmen zur Token- und Geheimnisverwaltung ein.

13. Speicherdauer und Löschung

- **Kontaktanfragen:** bis zur Erledigung und anschließend in der Regel bis zu 12 Monate.
- **Account-, Login- und Sicherheitslogs:** in der Regel bis zu 90 Tage, bei sicherheitsrelevanten Vorfällen bis zum Abschluss der Prüfung.
- **OAuth-Tokens und Integrationsverknüpfungen:** bis zur Trennung der Integration und anschließend in der Regel bis zu 30 Tage für technische Bereinigung.
- **Rechnungs-, Zahlungs- und steuerrelevante Unterlagen:** nach den gesetzlichen Aufbewahrungsfristen, abhängig von der Art der Unterlage regelmäßig sechs, acht oder zehn Jahre.
- **Backups:** rotierende Wiederherstellungspunkte mit einer maximalen regulären Aufbewahrungsdauer von 90 Tagen.
- **Kundendaten in der Plattform:** grundsätzlich nach Weisung des Kunden beziehungsweise nach Vertragsende und Ablauf vereinbarter Export- oder Übergabefristen.

14. Rechte betroffener Personen

Betroffene Personen haben im Rahmen der gesetzlichen Voraussetzungen das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch sowie Widerruf erteilter Einwilligungen mit Wirkung für die Zukunft.

Soweit wir Daten als Auftragsverarbeiter für einen Kunden verarbeiten, solltest du dich mit deinem Anliegen vorrangig an den jeweiligen Kunden als Verantwortlichen wenden. Wir unterstützen unsere Kunden bei der Erfüllung entsprechender Anfragen im Rahmen unserer vertraglichen Pflichten.

15. Beschwerderecht

Du hast das Recht, dich bei einer Datenschutz-Aufsichtsbehörde zu beschweren, wenn du der Ansicht bist, dass die Verarbeitung deiner personenbezogenen Daten gegen Datenschutzrecht verstößt.

30 Tage kostenlos testen