SYSTEMDATENSCHUTZ | SCHWEIZ

Datenschutzerklärung cardgate® System

Stand: 11. August 2026

1. Geltungsbereich und Verantwortlichkeit

Diese Datenschutzerklärung beschreibt die Bearbeitung von Personendaten im Zusammenhang mit der Website cardgate.io, dem Kontakt- und Demoformular sowie dem cardgate® Management-Portal und den zugehörigen Plattformdiensten.

Verantwortlich für Website, Kontaktanfragen, Portal-Konten und den eigenen Geschäftsbetrieb ist:

keynexis AG
Auf der Mauer 9
8001 Zürich, Schweiz
Telefon: +41 44 500 43 42
E-Mail: contact@keynexis.com

Bei Daten, die ein Kunde oder Anlagenbetreiber mit cardgate® für seine eigenen Zwecke bearbeitet - insbesondere Zutritts-, Nutzer- und Betriebsdaten -, ist in der Regel dieser Kunde verantwortlich. Die keynexis AG bearbeitet solche Daten nach dessen Weisungen als Auftragsbearbeiterin. Betroffene Personen können sich in diesem Fall direkt an den jeweiligen Anlagenbetreiber wenden.

2. Bearbeitete Daten und Zwecke

Wir bearbeiten Personendaten rechtmässig, verhältnismässig und nur für erkennbare Zwecke, insbesondere um:

- die Website und Plattform sicher und zuverlässig bereitzustellen;
- Anfragen zu beantworten, Demos zu organisieren und Geschäftsbeziehungen abzuwickeln;
- Nutzer zu authentifizieren, Berechtigungen zu verwalten und Missbrauch zu verhindern;
- cardgate®-Systeme zu konfigurieren, zu betreiben, zu warten und Support zu leisten;
- Sicherheits-, Zugriffs- und Änderungsvorgänge nachvollziehbar zu protokollieren; sowie
- gesetzliche Pflichten zu erfüllen und Ansprüche durchzusetzen oder abzuwehren.

3. Website und Server-Protokolle

Beim Aufruf der Website oder Plattform werden technisch notwendige Verbindungsdaten bearbeitet. Dazu können IP-Adresse, Datum und Uhrzeit, aufgerufene Adresse, Referrer, Browser- und Betriebssystemangaben, übertragene Datenmenge sowie Status- und Fehlermeldungen gehören. Diese Daten dienen der Auslieferung, Fehleranalyse, Systemsicherheit und Missbrauchsabwehr. Eine Zusammenführung zu Werbeprofilen findet nicht statt.

Die öffentliche Website setzt nach aktuellem Stand keine Analyse- oder Marketing-Cookies ein. Sie speichert lediglich die gewählte Sprache im lokalen Speicher des Browsers (cardgate.lang).

4. Kontakt- und Demoanfragen

Bei einer Anfrage bearbeiten wir Name und E-Mail-Adresse sowie freiwillig Firma, Nachricht, Quellseite und weitere übermittelte Angaben. Wir verwenden diese Daten zur Bearbeitung der Anfrage und für notwendige Anschlusskommunikation, nicht für Newsletter ohne separate Anmeldung.

Das Formular wird über unsere API verarbeitet und die Nachricht über Twilio SendGrid (Twilio Inc., USA) an uns zugestellt. Dabei werden die Formularangaben an Twilio übermittelt. Weitere Informationen enthält die Datenschutzerklärung von Twilio.

5. Externe Inhalte

Die Website lädt Schriftarten über Google Fonts. Dabei erhält Google insbesondere die IP-Adresse sowie technische Anfrageinformationen. Anbieter sind Google Ireland Limited (Irland) und verbundene Unternehmen, namentlich Google LLC (USA). Es werden durch Google Fonts nach unserem Kenntnisstand keine Cookies gesetzt. Weitere Informationen: Datenschutzerklärung von Google.

Auf der Kontaktseite ist eine Karte von OpenStreetMap eingebettet. Beim Laden des Kartenausschnitts können insbesondere IP-Adresse, Browserangaben und die aufgerufene Seite an die OpenStreetMap Foundation (Vereinigtes Königreich) und deren technische Dienstleister übermittelt werden. Weitere Informationen: Datenschutzerklärung der OpenStreetMap Foundation.

6. Management-Portal und cardgate®-Betrieb

Für Portal-Nutzer bearbeiten wir insbesondere Name, E-Mail-Adresse, Sprache, Passwort-Hash, Rollen, Mandantenzuordnungen, Anmelde- und Token-Daten sowie Erstellungs-, Änderungs- und Aktivitätszeitpunkte. Passwörter werden nicht im Klartext gespeichert.

Je nach Nutzung bearbeiten wir zudem Kunden-, Standort- und Anlagendaten, Gerätekennungen wie MAC-Adressen, Zeit- und Berechtigungsregeln, technische Zugangsdaten sowie Betriebs-, MQTT-, Audit- und Zutrittsereignisse. Ereignisdaten können Geräte- oder Medienkennungen, Zeitpunkte, Entscheidungen und technische Meldungen enthalten. Der Zugriff ist rollen- und mandantenbezogen beschränkt.

Zutrittsentscheidungen können automatisiert anhand der vom Anlagenbetreiber hinterlegten Berechtigungen und Zeitregeln erfolgen. Für die Regeln und deren Auswirkungen ist grundsätzlich der Anlagenbetreiber verantwortlich. Betroffene Personen können bei ihm eine Überprüfung verlangen.

Das Portal verwendet technisch notwendige Sitzungs- und Anmeldefunktionen. OAuth-Zustandsdaten werden vorübergehend im Sitzungsspeicher, Zugriffs- und Aktualisierungstoken im lokalen Browserspeicher und Darstellungspräferenzen lokal im Browser gespeichert. Beim Abmelden werden die Anmeldetoken im Browser gelöscht und serverseitig widerrufen; Darstellungspräferenzen können bestehen bleiben. Eine Login-Sitzung kann ohne frühere Abmeldung grundsätzlich bis zu 30 Tage bestehen.

7. Empfänger und Bekanntgabe ins Ausland

Personendaten erhalten nur Personen und Stellen, soweit dies für die genannten Zwecke erforderlich ist. Dazu gehören berechtigte Mitarbeitende, der zuständige Kunde oder Anlagenbetreiber, Hosting-, Datenbank-, E-Mail-, Support- und Sicherheitsdienstleister sowie Behörden, wenn eine gesetzliche Pflicht besteht.

Bearbeitungen können in der Schweiz, im Europäischen Wirtschaftsraum, im Vereinigten Königreich und in den USA erfolgen. Erfolgt eine Bekanntgabe in ein Land ohne vom Bundesrat anerkanntes angemessenes Datenschutzniveau, sorgen wir für einen geeigneten Schutz, insbesondere durch anerkannte Standarddatenschutzklauseln und erforderliche Zusatzmassnahmen, oder stützen uns auf eine gesetzliche Ausnahme. Auf Anfrage erteilen wir weitere Angaben zu den verwendeten Garantien.

8. Aufbewahrung und Sicherheit

Wir bewahren Personendaten nur so lange auf, wie es für den jeweiligen Zweck, die Vertragsabwicklung, Sicherheits- und Nachweisinteressen oder gesetzliche Pflichten erforderlich ist. Danach werden sie gelöscht oder anonymisiert. Für die einzelnen Datenkategorien gelten folgende Aufbewahrungsfristen beziehungsweise Kriterien:

- Website- und Server-Protokolle sowie technische Betriebs-, Audit- und Zugriffsdaten: sechs Monate ab Erfassung; danach werden sie gelöscht oder so anonymisiert, dass eine Zuordnung zu einer bestimmten oder bestimmbaren Person nicht mehr möglich ist.
- Portal-Konten, Kunden-, Standort-, Anlagen- und Konfigurationsdaten: für die Dauer des Kontos, des Vertragsverhältnisses oder des Anlagenbetriebs; danach nur so lange, wie sie für Vertragsabwicklung, Wiederherstellung, gesetzliche Pflichten oder die Geltendmachung beziehungsweise Abwehr von Ansprüchen erforderlich sind.
- Kontakt- und Demoanfragen: bis die Anfrage und die notwendige Anschlusskommunikation abgeschlossen sind; bei einer anschliessenden Geschäftsbeziehung oder gesetzlichen Nachweispflicht nach den dafür geltenden Fristen.
- Lokale Sitzungs- und Browserdaten: OAuth-Zustandsdaten bis zum Abschluss des Anmeldevorgangs, Anmeldetoken bis zur Abmeldung oder zum Ablauf der Sitzung von grundsätzlich höchstens 30 Tagen und Darstellungspräferenzen bis zu ihrer Löschung im Browser.

  Zugriffsereignisse des cardgate® Systems enthalten grundsätzlich technische Medien- oder Gerätekennungen, jedoch keine von cardgate® geführte Zuordnung dieser Kennungen zu Namen oder anderen unmittelbar identifizierenden Angaben der Karteninhaber. Eine indirekte Zuordnung kann nur durch die Zusammenführung mit separaten Zusatzinformationen des Kunden, Anlagenbetreibers oder eines Dritten entstehen. Portal-Auditdaten können dagegen Kennungen authentifizierter Nutzer enthalten. Eine Bekanntgabe durch die keynexis AG an Behörden erfolgt nur, wenn eine gesetzliche Grundlage oder eine rechtsverbindliche behördliche Anordnung besteht.

  Die sechsmonatige Aufbewahrung der technischen Log-, Audit- und Zugriffsdaten dient ausschliesslich der Systemsicherheit, Fehleranalyse, Missbrauchsabwehr und Nachvollziehbarkeit. Sie ist mit Datenminimierung, Zweckbindung, beschränkten Zugriffsrechten sowie anschliessender Löschung oder Anonymisierung ausgestaltet.

  Wir treffen angemessene technische und organisatorische Massnahmen, darunter verschlüsselte Übertragung, Zugriffsbeschränkungen, Mandantentrennung, Passwort-Hashing, Protokollierung und Datensicherung. Ein absoluter Schutz kann jedoch nicht garantiert werden.

9. Rechte betroffener Personen

Betroffene Personen können nach dem Schweizer Datenschutzgesetz insbesondere Auskunft, Berichtigung und - soweit die gesetzlichen Voraussetzungen erfüllt sind - Löschung oder Vernichtung, das Verbot einer Bearbeitung sowie die Herausgabe oder Übertragung ihrer Daten verlangen. Bei einer erheblich beeinträchtigenden automatisierten Einzelentscheidung können sie ihren Standpunkt darlegen und eine Überprüfung durch eine natürliche Person verlangen. Gesetzliche Aufbewahrungspflichten und Rechte Dritter bleiben vorbehalten.

Anfragen können mit einem geeigneten Identitätsnachweis an contact@keynexis.com gerichtet werden. Zudem besteht die Möglichkeit, sich an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu wenden.

10. Änderungen

Wir können diese Datenschutzerklärung anpassen, wenn sich Datenbearbeitungen oder rechtliche Anforderungen ändern. Es gilt die auf cardgate.io veröffentlichte aktuelle Fassung.