

Datenschutzerklärung QARD

Verantwortlicher

QARD GmbH

Otto-Kraus-Straße 10

90411 Nürnberg, Deutschland

E-Mail: hello@getqard.com

Website: getqard.com

Stand: 21. Januar 2026

Diese Datenschutzerklärung erläutert, wie wir personenbezogene Daten verarbeiten, wenn Sie eine digitale Karte über QARD nutzen, sowie wenn Sie unsere Website und Onboarding-Bereiche verwenden.

1. Kurzübersicht: Wer macht was

1.1 Kartenanbieter und QARD

Wenn Sie eine digitale Karte zu Apple Wallet oder Google Wallet hinzufügen, erhalten Sie diese Karte von einem konkreten Unternehmen, Verein oder einer Organisation (im Folgenden „Kartenanbieter“). Der Kartenanbieter entscheidet, welche Daten er abfragt, welche Vorteile gelten und welche Kommunikation stattfinden soll.

Regelmodell

- Der Kartenanbieter ist Verantwortlicher für die Verarbeitung im Rahmen seines Kundenprogramms.
- QARD verarbeitet Daten im Auftrag des Kartenanbieters, um die Karte technisch bereitzustellen, zu aktualisieren und Wallet-Funktionen zu ermöglichen.

Auftragsverarbeitung (Art. 28 DSGVO)

Soweit QARD personenbezogene Daten für den Kartenanbieter verarbeitet, erfolgt dies auf Grundlage eines Auftragsverarbeitungsvertrags gemäß Art. 28 DSGVO und ausschließlich nach Weisung des Kartenanbieters.

Zusätzlich verarbeiten wir bestimmte Daten als eigener Verantwortlicher, soweit dies für den Betrieb der Plattform erforderlich ist, insbesondere für IT-Sicherheit, Missbrauchsprävention, Fehleranalyse, Support und die Bereitstellung unserer Website.

1.2 Wallet-Anbieter

Apple Wallet und Google Wallet werden von Apple bzw. Google bereitgestellt. Diese Anbieter verarbeiten Daten in eigener Verantwortung, wenn Sie deren Wallet-Funktionen nutzen. Bitte beachten Sie zusätzlich die Datenschutzhinweise der jeweiligen Anbieter.

2. Welche Daten wir verarbeiten

2.1 Technische Kartendaten und IDs

Wir verarbeiten, je nach Nutzung und Konfiguration, insbesondere:

- interne Pass-ID (Primärschlüssel) und Seriennummer der Karte
- Zuordnung der Karte zum Kartenanbieter über campaign_id und Kundenzuordnung
- Zeitstempel wie created_at, last_updated_at, last_scanned_at
- Apple: technische Push-Tokens, soweit erforderlich, um Pass-Updates über Apple APNs auszulösen
- Google: Referenzen zum Google-Wallet-Objekt, soweit erforderlich, um Updates über die Google Wallet API auszulösen

2.2 Endkundendaten (falls der Kartenanbieter diese abfragt)

Je nach Einstellung des Kartenanbieters können zusätzlich gespeichert werden:

- Name
- E-Mail
- Telefonnummer
- Geburtsdatum

Diese Daten werden nur erhoben, wenn der Kartenanbieter diese Felder in seinem Programm aktiv nutzt und die Daten von Ihnen eingegeben werden. Der Kartenanbieter kann diese Daten in seinem Dashboard einsehen und im Rahmen seines Programms verarbeiten.

2.3 Einwilligungen und Nachweisprotokolle (Marketing-Opt-in)

Wenn Sie „Vorteile aktivieren“ auswählen, speichern wir den Status und den Nachweis, damit Marketing-Inhalte nur bei Opt-in ausgespielt werden:

- consent_marketing (true oder false)
- consent_marketing_at (Zeitstempel)
- consent_source (z. B. popup_onboarding)
- consent_text_version und consent_text_hash (Version und Hash des Einwilligungstextes)

Diese Nachweise werden benötigt, um Einwilligungen nachvollziehbar zu dokumentieren und im Streitfall belegen zu können, dass Marketing-Push nur an Opt-in-Empfänger ging.

2.4 Standort und Geofencing

Wir speichern keine Standortdaten der Endnutzer.

Geofencing funktioniert so, dass Koordinaten des Kartenanbieters im Pass hinterlegt sein können und das Betriebssystem Ihres Geräts die Anzeige lokal steuert. Unsere Systeme erhalten dabei keine Standortdaten und erstellen keine Bewegungsprofile.

2.5 Protokolldaten (Logs)

Beim Betrieb der Plattform entstehen technische Logs bei Hosting- und Datenbankbetrieb. Diese können IP-Adresse, Zeitstempel, Geräte- und Browserinformationen enthalten. Wir nutzen sie für IT-Sicherheit, Stabilität, Fehleranalyse und Missbrauchsprävention.

3. Zwecke und Rechtsgrundlagen

3.1 Bereitstellung und Verwaltung der Karte

Zwecke

- Karte ausliefern und verwalten
- Kartendaten aktualisieren
- Funktionen wie Punkte, Stempel, Coupons, Statuslevel technisch abbilden

Rechtsgrundlagen

- Vertragserfüllung bzw. Durchführung, Art. 6 Abs. 1 lit. b DSGVO
- berechtigtes Interesse an sicherem, stabilem Betrieb, Art. 6 Abs. 1 lit. f DSGVO

3.2 Wallet-Push: Service-Inhalte und Marketing-Inhalte

Es gibt zwei Kategorien:

- Service- und Funktionsinformationen, die der Nutzung der Karte dienen
- Angebote und Vorteile, die werbliche Inhalte sein können

Angebote und Vorteile werden nur verarbeitet und ausgespielt, wenn ein Opt-in vorliegt.

Rechtsgrundlage ist dann Einwilligung, Art. 6 Abs. 1 lit. a DSGVO. Ein Widerruf muss so einfach sein wie das Opt-in.

Wichtig: Der Kartenanbieter erstellt Inhalte und beantragt den Versand über sein Dashboard. QARD vermittelt den Versand technisch und kann Anfragen aus technischen, sicherheitsbezogenen oder compliancebezogenen Gründen genehmigen oder ablehnen.

3.3 Personalisierung, z. B. Geburtstag

Wenn der Kartenanbieter Geburtstagsfunktionen aktiviert und dafür ein Geburtsdatum abfragt, erfolgt die Verarbeitung für diesen Zweck im Rahmen des Programms des Kartenanbieters. QARD verarbeitet diese Daten technisch zur Bereitstellung der Funktion.

3.4 Support

Wenn Sie uns per E-Mail kontaktieren, verarbeiten wir die übermittelten Daten zur Bearbeitung Ihrer Anfrage.

Rechtsgrundlagen

- Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an Support)
- je nach Fall Art. 6 Abs. 1 lit. b DSGVO

3.5 Website, Onboarding-Bereiche und technisch notwendige Speicherung

Für Login und Sessions nutzen wir technisch notwendige Mechanismen (z. B. Supabase Auth). Dafür können Cookies oder ähnliche Speicherungen erforderlich sein.

Für technisch erforderliche Speicherung ist nach dem TDDDG keine Einwilligung nötig, sofern sie für die Bereitstellung des Dienstes erforderlich ist.

Im Onboarding zum Hinzufügen einer Karte setzen wir aktuell keine Marketing-Tracker und keine Webanalyse-Tools ein.

3.6 Pflicht zur Bereitstellung bestimmter Daten

Bestimmte Daten sind erforderlich, um die Karte technisch bereitzustellen und zu aktualisieren (z. B. Pass-ID/Seriennummer und technische Wallet-Identifikatoren). Ohne diese Daten kann die Karte nicht bereitgestellt oder aktualisiert werden.

4. Empfänger der Daten

4.1 Kartenanbieter

Der jeweilige Kartenanbieter erhält Zugriff auf die Daten, die im Rahmen seines Programms erhoben werden, einschließlich Name, E-Mail, Telefonnummer und Geburtsdatum, sofern diese Felder erhoben wurden.

4.2 Dienstleister und Unterauftragsverarbeiter

Wir nutzen folgende Dienstleister:

- Vercel für Hosting und Serverless Funktionen
 - Supabase (PostgreSQL) als Datenbank, Projektregion Frankfurt
 - Resend für E-Mail-Versand (nur, wenn E-Mail im jeweiligen Prozess genutzt wird)
 - Apple APNs und Google Wallet API für technische Pass-Updates
-

5. Übermittlung in Drittländer (z. B. USA)

Ein Teil unserer Dienstleister ist in den USA ansässig oder nutzt globale Infrastrukturen. Dadurch kann eine Verarbeitung in Drittländern, insbesondere den USA, nicht vollständig ausgeschlossen werden.

Für solche Übermittlungen nutzen wir geeignete Garantien, insbesondere Standardvertragsklauseln und, soweit anwendbar, den Angemessenheitsbeschluss zum EU-US Data Privacy Framework für teilnehmende Unternehmen.

6. Löschfristen: So machen wir es konkret

6.1 Karten und Endkundendaten in „passes“

- Solange die Karte aktiv genutzt wird, speichern wir die Daten für die Bereitstellung des Programms.
- Wenn eine Karte 24 Monate lang keine Aktivität mehr hat (kein Update, kein Scan, keine Nutzung im System, gemessen an last_scanned_at und last_updated_at), wird sie als inaktiv markiert.
- 30 Tage nach Inaktiv-Markierung löschen wir die personenbezogenen Endkundendatenfelder (Name, E-Mail, Telefon, Geburtstag) oder anonymisieren sie, sofern der Kartenanbieter keine längere Speicherung anfordert und keine gesetzlichen Pflichten entgegenstehen.
- Technische IDs (Pass-ID, Seriennummer, Merchant-Zuordnung) können wir in pseudonymisierter Form länger behalten, soweit dies für Systemintegrität, Missbrauchsprävention und Nachweiszwecke erforderlich ist.

6.2 Marketing-Opt-in-Nachweise (consent logs)

- Opt-in-Nachweise speichern wir 3 Jahre ab Ende des Jahres, in dem die Karte zuletzt aktiv war oder der Opt-in-Status zuletzt geändert wurde.

Begründung: Nachweis und Rechtsverteidigung orientieren sich an der regelmäßigen Verjährung, die in Deutschland typischerweise 3 Jahre beträgt, mit Fristbeginn häufig zum Jahresende.

6.3 Technische Logs

- Sicherheits- und Systemlogs speichern wir in der Regel 30 Tage, bei Sicherheitsvorfällen ggf. länger, solange dies zur Aufklärung erforderlich ist.

6.4 Support-Anfragen

- Support-Kommunikation speichern wir 12 Monate nach Abschluss des Vorgangs, sofern keine gesetzliche Pflicht oder ein konkreter Streitfall eine längere Aufbewahrung erfordert.

6.5 B2B-Vertrags- und Abrechnungsdaten (Merchants)

- Handels- und steuerrechtliche Unterlagen können länger gespeichert werden, soweit gesetzliche Aufbewahrungspflichten bestehen.

7. Ihre Rechte

Sie haben insbesondere das Recht auf:

- Auskunft (Art. 15 DSGVO)
- Berichtigung (Art. 16 DSGVO)
- Löschung (Art. 17 DSGVO)
- Einschränkung der Verarbeitung (Art. 18 DSGVO)

- Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruch gegen Verarbeitung auf Basis berechtigter Interessen (Art. 21 DSGVO)
- Widerruf einer Einwilligung jederzeit mit Wirkung für die Zukunft (Art. 7 Abs. 3 DSGVO)

Der Widerruf muss so einfach sein wie die Erteilung.

Für Anliegen, die das Kundenprogramm betreffen, ist der Kartenanbieter meist der schnellste Ansprechpartner. Sie können sich aber auch an uns wenden. Wir unterstützen technisch oder leiten weiter, soweit möglich: hello@getqard.com

Sie haben außerdem das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren.

8. Wallet-Mitteilungen deaktivieren: So geht es

Sie können Wallet-Mitteilungen in den Einstellungen Ihres Geräts deaktivieren, entweder global oder für eine bestimmte Karte, abhängig von den Funktionen Ihres Betriebssystems und Ihrer Wallet-App.

Wenn Sie Unterstützung benötigen oder die Vorteile-Funktion für eine bestimmte Karte deaktiviert werden soll, schreiben Sie an hello@getqard.com.

9. Keine Tracking-Tools im Karten-Onboarding

Im Onboarding zum Hinzufügen einer Karte setzen wir aktuell keine Marketing-Pixel, kein Retargeting und keine Webanalyse-Tools ein.

Sollten wir künftig Analyse- oder Marketing-Tools auf getqard.com einsetzen, holen wir, soweit erforderlich, vorher eine Einwilligung nach TDDDG und DSGVO ein.

10. Automatisierte Entscheidungen

Eine automatisierte Entscheidungsfindung oder Profiling im Sinne von Art. 22 DSGVO findet nicht statt.

11. Sicherheit

Wir setzen technische und organisatorische Maßnahmen ein, um Daten zu schützen, insbesondere Zugriffskontrollen, Rollen- und Rechtekonzepte, Verschlüsselung bei der Übertragung sowie Protokollierung zur Missbrauchsprävention.

12. Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist derzeit nicht bestellt.

13. Kontakt

QARD GmbH

Otto-Kraus Straße 10

90411 Nürnberg, Deutschland

E-Mail: hello@getqard.com