

Datenschutzerklärung für die App "Tario"

1. Verantwortlicher für die Datenverarbeitung

Verantwortlich im Sinne der Datenschutz-Grundverordnung (DSGVO) und anderer nationaler Datenschutzgesetze ist:

Marcel Giesen

Am Alten Stadion 12

42697 Solingen

Deutschland

E-Mail: tario@posteo.eu

2. Grundprinzipien unserer Datenverarbeitung (Privacy by Design)

Die Tario-App wurde nach dem "Offline-First"-Prinzip entwickelt. Das bedeutet: Ihre Daten gehören Ihnen. Die App funktioniert grundsätzlich auch ohne das Anlegen eines klassischen Nutzerkontos (Gast-Modus). Wir erheben nur die Daten, die für die Funktionalität der App (das Teilen und Synchronisieren von Reiseausgaben) technisch zwingend erforderlich sind.

3. Welche Daten wir verarbeiten und warum

a) Lokale Speicherung (Offline-Nutzung):

Um Ihnen eine nahtlose Nutzung auch ohne aktive Internetverbindung zu ermöglichen, werden Ihre Eingaben (Reisenamen, Ausgabenbeträge, Währungen, beteiligte Personen) zunächst lokal auf Ihrem Endgerät (Smartphone oder lokaler Web-Browser) gespeichert. Diese Speicherung erfolgt über die Datenbanktechnologie "Hive". Die lokal gespeicherten Daten werden durch moderne Verschlüsselungsverfahren (AES) kryptografisch abgesichert. In diesem Zustand haben wir keinen Zugriff auf Ihre Daten.

b) Cloud-Synchronisation & Gast-Modus:

Damit Sie Reisen mit anderen Personen teilen können, synchronisiert die App Ihre lokalen Daten über eine verschlüsselte Verbindung (SSL/TLS) mit unserer Cloud-Datenbank, sobald eine Internetverbindung besteht. Im Gast-Modus (Anonyme Nutzung) generiert die App hierfür eine rein zufällige, anonyme Identifikationsnummer (UUID v4). Es werden keine Klardaten wie Ihr echter Name, Ihre E-Mail-Adresse oder Ihre Telefonnummer an uns übermittelt. Die Verarbeitung erfolgt auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung).

c) Prüfung der Internetverbindung:

Die App prüft lokal auf Ihrem Gerät den Status Ihrer Netzwerkverbindung, um den Datenabgleich im Hintergrund zu steuern. Dabei werden keine Standortdaten oder Details über Ihr WLAN an uns gesendet.

d) Server-Logfiles beim Web-Hosting und bei der Synchronisation:

Wir hosten unsere Web-Applikation bei der Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen (nachfolgend „Hetzner“). Wenn Sie unsere Web-App besuchen oder die mobile App Daten mit unserer Cloud synchronisiert, erfasst der Server technisch bedingt vorübergehend Zugriffsdaten in sogenannten Server-Logfiles. Dazu gehören unter anderem Ihre IP-Adresse, Browsertyp und Browserversion, verwendetes Betriebssystem, Datum und Uhrzeit der Anfrage sowie die übertragene Datenmenge. Eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen. Diese Speicherung erfolgt auf Grundlage unseres berechtigten Interesses (Art. 6 Abs. 1 lit. f DSGVO) an einer möglichst zuverlässigen Darstellung und der Aufrechterhaltung der Server-Sicherheit. Die IP-Adressen werden nach wenigen Tagen automatisiert gelöscht. Wir haben einen Vertrag zur Auftragsverarbeitung (AVV) mit Hetzner geschlossen.

e) Registrierte Nutzer (Magic Link Login):

Wenn Sie sich entscheiden, ein festes Nutzerkonto in der App anzulegen, erheben und speichern wir ausschließlich Ihre E-Mail-Adresse. Wir verzichten aus Sicherheits- und Datenschutzgründen bewusst auf die Speicherung von Passwörtern. Stattdessen nutzen wir ein "Magic Link"-Verfahren: Bei der Anmeldung senden wir einen temporären, verschlüsselten Zugangslink an Ihre E-Mail-Adresse, mit dem Sie sich authentifizieren. Ihre E-Mail-Adresse ist zwingend erforderlich, um Ihr Konto zuzuordnen und geräteübergreifende Synchronisationen zu ermöglichen. Die Verarbeitung erfolgt auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO. Wir nutzen Ihre E-Mail-Adresse nicht für Werbe-Newsletter.

4. Eingesetzte Dienstleister & Drittlandtransfer

Um die App technisch betreiben zu können und die Backend-Infrastruktur bereitzustellen, nutzen wir den Dienst Supabase (Supabase Inc., 970 16th Street, San Francisco, CA 94107, USA). Supabase verarbeitet für uns die Authentifizierung (z.B. Login via E-Mail/Magic Link) und stellt die Datenbank-Infrastruktur (PostgreSQL) zur Speicherung und Synchronisation der Reise- und Ausgabendaten bereit. Die physische Speicherung dieser Daten erfolgt auf Servern in Frankfurt am Main, Deutschland / der Europäischen Union (eu-central-1). Wir haben mit Supabase einen Vertrag zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO geschlossen. Sofern Daten durch Supabase in den USA verarbeitet werden, stützen wir dies auf den Angemessenheitsbeschluss der EU-Kommission (EU-US Data Privacy Framework) bzw. auf Standardvertragsklauseln (SCC) der EU-Kommission. Weitere Informationen zum Datenschutz bei Supabase finden Sie unter: <https://supabase.com/privacy>.

5. Externe Links und Spenden (Ko-fi)

In der App bieten wir die Möglichkeit, unser Projekt über die Plattform Ko-fi freiwillig finanziell zu unterstützen (<https://ko-fi.com/splittr>). Wenn Sie auf diesen Link klicken, verlassen Sie unsere App und werden auf die Server von Ko-fi weitergeleitet. Ab diesem Moment gilt die Datenschutzerklärung von Ko-fi (<https://more.ko-fi.com/privacy>). Wir erheben oder speichern selbst keine Zahlungsdaten von Ihnen. Für die Verarbeitung Ihrer Zahlungs- und Nutzerdaten auf Ko-fi ist ausschließlich der Betreiber der Plattform verantwortlich (Ko-fi Labs Ltd.).

6. Speicherdauer und Löschung

Wir speichern Ihre Daten nur so lange, wie es für die Bereitstellung der App-Funktionen notwendig ist.

- **Logische Löschung (Soft-Delete):** Wenn Sie eine Ausgabe oder Reise in der App löschen, wird diese in der Datenbank mit einem "Gelöscht"-Status markiert und auf Ihrem Bildschirm ausgeblendet. Dies dient dem Schutz vor versehentlichem Datenverlust und der Synchronisations-Stabilität der Offline-Architektur.
- **Vollständige Löschung & Account-Löschung:** Wenn Sie die App als Gast nutzen und deinstallieren (oder die Web-App-Daten im Browser löschen), werden alle lokalen Daten auf Ihrem Gerät gelöscht. Wenn Sie ein registriertes Nutzerkonto besitzen, reicht die Deinstallation der App nicht aus, um Ihre Daten auf unseren Servern zu löschen. Sie finden in den Einstellungen der App einen Button "Konto löschen". Wenn Sie diesen betätigen, wird Ihr Konto unwiderruflich aus unserer Authentifizierungs-Datenbank gelöscht (Art. 17 DSGVO). Ihre bisherigen Ausgaben und Reisen verbleiben in diesem Fall in anonymisierter Form in den geteilten Gruppen, damit die Abrechnungen der anderen Reiset Teilnehmer nicht zerstört werden.
- **Verwaiste Daten im Gast-Modus:** Da wir Ihre Daten im Gast-Modus ohne Ihre gerätespezifische UUID nicht manuell ausfindig machen können, haben eine automatisierte Löschroutine eingerichtet. Reisen und Ausgaben von Gastnutzern, die über einen Zeitraum von 30 Tagen vollständig inaktiv waren, werden als verwaiste Daten eingestuft und unwiderruflich aus unserer Cloud-Datenbank gelöscht (Art. 5 Abs. 1 lit. e DSGVO).

7. Ihre Rechte als betroffene Person

Gemäß der DSGVO haben Sie das Recht auf Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18), Datenübertragbarkeit (Art. 20) und Widerspruch (Art. 21).

- **Hinweis zum Gast-Modus:** Da wir im Gast-Modus keine identifizierenden Daten (wie Namen oder E-Mails) von Ihnen besitzen, können wir Anfragen nur bearbeiten, wenn Sie uns Ihre gerätespezifische, anonyme UUID mitteilen.

- **Recht auf Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO):** Sofern die Datenverarbeitung auf Ihrer Einwilligung beruht, haben Sie das Recht, diese jederzeit mit Wirkung für die Zukunft zu widerrufen.
- **Recht auf Beschwerde (Art. 77 DSGVO):** Sie haben das Recht auf Beschwerde bei einer Datenschutz-Aufsichtsbehörde, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer Daten gegen die DSGVO verstößt.

Privacy Policy for the "Tario" App

1. Data Controller

The controller within the meaning of the General Data Protection Regulation (GDPR) and other national data protection laws is:

Marcel Giesen

Am Alten Stadion 12

42697 Solingen

Germany

E-Mail: tario@posteo.eu

2. Basic Principles of Data Processing (Privacy by Design)

The Tario app was developed following the "offline-first" principle. This means: Your data belongs to you. The app generally functions without creating a classic user account (Guest Mode). We only collect data that is technically absolutely necessary for the functionality of the app (sharing and synchronizing travel expenses).

3. What Data We Process and Why

a) Local Storage on the Device (Hive / Offline Use):

To allow you to use the app seamlessly even without an active internet connection, your inputs (trip names, expense amounts, currencies, involved persons) are initially stored locally on your device (smartphone or local web browser). This storage uses the "Hive" database technology. The locally stored data is cryptographically secured using modern encryption methods (AES). In this state, we have no access to your data.

b) Cloud Synchronization & Guest Mode:

To allow you to share trips with other people, the app synchronizes your local data via an encrypted connection (SSL/TLS) with our cloud database as soon as an internet connection is established. In Guest Mode (anonymous use), the app generates a purely random, anonymous identification number (UUID v4) for this purpose. No clear text data such as your real name, email address, or phone number is transmitted to us. Processing is based on Art. 6 (1) (b) GDPR (performance of a contract).

c) Internet Connection Check:

The app locally checks your network connection status to manage background data synchronization. No location data or details about your Wi-Fi are sent to us.

d) Server Log Files during Web Hosting and Synchronization:

We host our web application with Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany (hereinafter "Hetzner"). When you visit our web app or the mobile app synchronizes data with our cloud, the server temporarily collects access data in so-called server log files for technical reasons. This includes, among other things, your IP address, browser type and version, operating system used, date and time of the request, and the amount of data transferred. This data is not merged with other data sources. This storage is based on our legitimate interest (Art. 6 (1) (f) GDPR) in ensuring the most reliable presentation possible and maintaining server security. IP addresses are automatically deleted after a few days. We have concluded a Data Processing Agreement (DPA) with Hetzner.

e) Registered Users (Magic Link Login):

If you choose to create a registered user account in the app, we exclusively collect and store your email address. For security and privacy reasons, we deliberately do not store passwords. Instead, we use a "Magic Link" procedure: When logging in, we send a temporary, encrypted access link to your email address, which you use to authenticate yourself. Your email address is strictly necessary to identify your account and enable cross-device synchronization. Processing is based on Art. 6 (1) (b) GDPR. We do not use your email address for promotional newsletters.

4. Service Providers & Third-Country Transfers (Supabase)

To technically operate the app and provide the backend infrastructure, we use the service Supabase (Supabase Inc., 970 16th Street, San Francisco, CA 94107, USA). Supabase processes authentication for us (e.g., login via email/magic link) and provides the database infrastructure (PostgreSQL) to store and synchronize trip and expense data. The physical storage of this data takes place on servers located in Frankfurt am Main, Germany / the European Union (eu-central-1). We have concluded a Data Processing Agreement (DPA) with Supabase in accordance with Art. 28 GDPR. If data is processed by Supabase in the USA, we base this on the adequacy decision of the EU Commission (EU-US Data Privacy

Framework) or on Standard Contractual Clauses (SCC) of the EU Commission. Further information on data protection at Supabase can be found at: <https://supabase.com/privacy>.

5. External Links and Donations (Ko-fi)

In the app, we offer the opportunity to voluntarily support our project financially via the Ko-fi platform (<https://ko-fi.com/splittr>). If you click on this link, you leave our app and will be redirected to the Ko-fi servers. From this moment on, the Ko-fi privacy policy applies (<https://more.ko-fi.com/privacy>). We do not collect or store any of your payment data ourselves. The operator of the platform (Ko-fi Labs Ltd.) is solely responsible for processing your payment and user data on Ko-fi.

6. Storage Duration and Deletion

We only store your data for as long as necessary to provide the app functions.

- **Logical Deletion (Soft Delete):** If you delete an expense or trip in the app, it is marked with a "deleted" status in the database and hidden on your screen. This serves to protect against accidental data loss.
- **Complete Deletion & Account Deletion:** If you use the app as a guest and uninstall it, all local data on your device will be deleted. If you have a registered user account, simply uninstalling the app is not sufficient to delete your data on our servers. You will find a "Delete Account" button in the app's settings. By executing this action, your email address will be irrevocably deleted from our authentication database (Art. 17 GDPR). Your previous expenses and trips will remain in an anonymized form within the shared groups, so that the financial settlements of the other trip participants are not destroyed.
- **Orphaned Data in Guest Mode:** Since we cannot manually locate your data in Guest Mode without your device-specific UUID, we have implemented an automated deletion routine. Trips and expenses of guest users that have been completely inactive for a period of 30 days are classified as orphaned data and irrevocably deleted from our cloud database (Art. 5 (1) (e) GDPR).

7. Your Rights as a Data Subject

According to the GDPR, you have the right to access (Art. 15), rectification (Art. 16), erasure (Art. 17), restriction of processing (Art. 18), data portability (Art. 20), and objection (Art. 21).

- **Note on Guest Mode:** Since we do not possess any identifying data (like names or emails) from you in Guest Mode, we can only process requests if you provide us with your device-specific, anonymous UUID.
- **Right to Withdraw Consent (Art. 7 (3) GDPR):** If data processing is based on your consent, you have the right to withdraw this at any time with effect for the future.
- **Right to Lodge a Complaint (Art. 77 GDPR):** You have the right to lodge a complaint with a data protection supervisory authority if you believe that the processing of your data violates the GDPR.