Privacy policy

How Trepup collects, uses, and protects your data

Issued by Trepup.com AG, Zug | Effective 1 December 2026

This is the Privacy policy ("Policy") for Trepup. The short version: we collect what we need to run the Platform and nothing more. Your data is stored in Frankfurt, Germany; when an AI feature runs, the Content it needs is sent to Anthropic for processing, under its data processing agreement and transfer impact assessment. Your card data never touches our servers. Your Account is passwordless - there are no passwords to steal because there are no passwords. We do not sell your data. We do not use your Content to train AI models. We do not track you across the internet. You can export or delete everything at any time. Swiss law governs this Policy. If something goes wrong, the courts of Zug, Switzerland decide.

This Policy overlaps with the Terms of service on four topics: AI data processing, sign-up data collection, Content limits, and Account deletion timelines. Where both documents address the same topic, this Policy is canonical for data processing and collection, and the Terms of service are canonical for contractual rights and feature limits. If the two documents conflict, the Terms of service govern contractual obligations and this Policy governs data protection obligations.

1. Who we are

In brief: We are Trepup.com AG, a Swiss company in Zug. Contact privacy@trepup.com for data protection matters.

Trepup.com AG ("Trepup," "we," "us") is the data controller for your personal data. We are a company registered in Zug, Switzerland (CHE-350.031.599), headquartered at Poststrasse 30, CH-6300 Zug.

For privacy inquiries, contact our privacy team at privacy@trepup.com.

Trepup has not appointed a separate Data Protection Officer under GDPR Article 37 or the Swiss FADP because Trepup does not process special categories of personal data on a large scale and does not carry out large-scale systematic monitoring. This position is reviewed annually. All data protection matters are handled by privacy@trepup.com.

2. What we collect

In brief: We collect your email, name, handle, date of birth, gender, and country at sign-up. We never collect passwords, GPS, biometrics, or browsing history outside Trepup.

Principle

Trepup follows the GDPR data minimisation principle (Article 5(1)(c)). We collect only the personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed. Every field listed below has a stated purpose. If we cannot state the purpose, we do not collect the field.

For example, Trepup never asks for your GPS location - the feed, search, and boost targeting work from the country you give at sign-up.

Account data you provide

When you create an Account and complete your profile, we collect the following fields. This is the complete list - we do not collect anything beyond what is shown here.

Field	When collected	Why
Email address	Sign-up (Step 0)	Authentication (magic link), Account recovery, transactional emails.
Handle	Profile setup (Step 4)	Your unique identifier on Trepup. Appears in your profile URL. 3-20 characters.
First name, last name	Profile setup (Step 4)	Display name (always first name + last name). Profile identification. Maximum 30 characters each.
Date of birth	Profile setup (Step 4)	Age verification (18+ required), and, only in aggregate as an age band, audience demographics in analytics. Not displayed publicly.
Gender	Profile setup (Step 4)	Boost targeting, and audience demographics in analytics for Users and Stores, in aggregate only. Options: male, female, non-binary, undisclosed. Required field with opt-out via undisclosed.
Country	Profile setup (Step 4)	Boost targeting by country, audience demographics in analytics for Users and Stores in aggregate only, and the consumer protections that apply to you. Suggested from your device's region setting, never from your location; you confirm or change it. Required field.
Avatar image	Optional, any time	Profile photo. If not set, a coloured initial is generated from your name.
Avatar colour	Account creation (automatic)	Hash-based colour assignment from a 55-colour palette. Used when no avatar image is set.
Bio	Optional, any time	Profile description. Maximum 150 characters for both Users and Stores.

Data received from Google

When you authenticate with Google OAuth ("Continue with Google"), we receive your email address and display name from Google. Google does not share your Google account password with us. If your Google email matches an existing Trepup Account, you are signed in to that Account. If it does not, a new Account is created using the email address provided by Google.

Data received from Apple

When you sign in with Apple ("Continue with Apple"), we receive the email address Apple shares for you - your own address, or a private relay address if you choose to hide yours - and, the first time you sign in only, the name you allow Apple to share. Apple does not share your Apple Account password with us. If that email matches an existing Trepup Account, you are signed in to that Account. If it does not, a new Account is created using it.

Sign-in providers. You may sign in with a magic link, with Google, or with Apple. Google and Apple are controllers of their own services and receive only that you signed in to Trepup. If you use Apple's private relay, the relay address is your address with us for every purpose, including the magic link and every notice.

Store data

If you create a Store, we additionally collect: Store name (maximum 50 characters), category (from the 33 categories of the Trepup category taxonomy), location address, contact information, opening hours, an about section (maximum 1,000 characters), and its Assistant knowledge - what the Store tells Trep about itself, for Trep to answer its buyers (up to 8,000 characters, and up to 20 questions and answers of up to 500 characters each). Products and services you list include titles (maximum 70 characters), descriptions (maximum 5,000 characters), prices, images, videos, and audio.

If you buy or sell - that is, if you move money on Trepup in either direction - you first complete verification with our payment partner, Stripe: through Stripe Identity to buy, and through Stripe's seller onboarding to sell. Your identity document and, where used, a selfie match are processed by Stripe. Trepup stores only the resulting status (unverified, pending, identity verified, entity verified, or failed), the Stripe verification session reference, and the date.

Content you create

Posts (captions up to 2,200 characters), reviews (up to 4,000 characters), review responses (up to 4,000 characters), messages (up to 1,000 characters), and comments (up to 2,200 characters). All Content limits are enforced at the database level.

Calls. Voice and video calls in the inbox connect the two devices directly, encrypted end to end, and nothing said or shown in a call is recorded or stored. For each call Trepup keeps only its thread, the caller and the person called, whether it was voice or video, when it started, was answered and ended, and how it ended (completed, declined, missed or failed), with one line in the thread recording that outcome. To find the direct route, each device asks Cloudflare's public STUN server for its own public address, so Cloudflare, already our network partner, sees the device's IP address when a call is set up - and nothing of the call itself. No relay carries a call; if one is ever added, it will be named in this Policy and the Data processing policy before it carries one.

Data we collect automatically

When you use Trepup, we automatically collect: IP address, device type, browser type and version, operating system, pages visited, features used, timestamps, and referral source. We use this data for Platform operation, abuse prevention, and aggregate analytics.

What we collect but never display

Several fields are collected for specific operational purposes but are never shown on your profile, in search results, or anywhere visible to other users. Date of birth is used for age verification (18+ requirement), for promotions matched to an age range, and, only in aggregate as an age band, for the audience demographics shown in analytics, and is never displayed. Country is used for Boost targeting, for audience demographics in analytics in aggregate only, and for the consumer protections that apply to you, and is never displayed. Gender is used for Boost targeting and, only in aggregate, for the audience demographics shown in analytics for Users and Stores - never for any one person - and is never displayed. Email address is used for authentication and transactional

emails and is never displayed on public surfaces. Avatar colour (the internal palette value) is used for rendering your default avatar and is never exposed as a data point.

What we do not collect

Trepup does not collect: passwords (we are passwordless), browsing history outside Trepup, contacts or address books, precise GPS location, biometric data (any selfie match in identity verification runs inside Stripe Identity and Trepup receives only the outcome), card data (Trepup holds only the Stripe payment token), health data, political affiliation, social security or national identity numbers, religious or philosophical beliefs, trade union membership, genetic data, or data concerning a person's sex life or sexual orientation.

Statutory and contractual requirements

Provision of your email address is a contractual requirement for Account creation. You cannot create an Account without it. Handle, first name, last name, date of birth, gender, and country are required to complete your profile and access the feed. All other fields are voluntary. If you do not provide the required fields, you will not be able to use the corresponding features.

3. How we use your data

In brief: Every use has a stated purpose and a GDPR legal basis. We do not sell your data or share it with advertisers.

We use your data only for the purposes listed in this table. Each purpose has a specific GDPR legal basis.

Purpose	Data used	Legal basis (GDPR)
Account creation and authentication	Email, handle, name, date of birth, gender, country	Performance of contract (Article 6(1)(b))
Profile display and social interaction	Name, handle, avatar image, bio, website link	Performance of contract (Article 6(1)(b))
Store operation and commerce	Store data, product and service listings, orders	Performance of contract (Article 6(1)(b))
Payment processing	Stripe payment token (not card data), billing address	Performance of contract (Article 6(1)(b))
Feed personalisation and recommendations	Usage data, interaction history, follows, saves	Legitimate interest (Article 6(1)(f)) - providing relevant Content
AI features (captions, search, Store reviews)	Content submitted to AI feature at time of use	Performance of contract (Article 6(1)(b))

Purpose	Data used	Legal basis (GDPR)
Boost advertising delivery	Country, age range, gender, whether you are a person or a Store, and the category you are viewing; for personalised promotions, the categories you engage with, whether you buy retail or wholesale, products or services, and the media you watch - never health	Legitimate interest (Article 6(1)(f)) for country, age range, gender, person or Store, and the category you are viewing - you may object in Settings, and promotions then never use them for you; consent (Article 6(1)(a)) for personalised promotions where the law asks first - the EEA, the United Kingdom, Switzerland, India, Brazil, China, South Korea and Turkey - asked once at sign-up and changed in Settings; elsewhere personalised promotions are on until you turn them off in Settings. Health is never used. A Store is a business: its interests are always used
Audience analytics (Users and Stores)	Gender, age band, and country of an Actor's audience, in aggregate only - never shown for any one person, and only for audiences of at least 100 people	Legitimate interest (Article 6(1)(f)) - giving every Actor an understanding of their audience
Platform security and abuse prevention	IP address, device and browser type, usage patterns	Legitimate interest (Article 6(1)(f)) - protecting users
Identity verification to move money	Verification status, Stripe verification session reference, date; documents and any selfie match stay with Stripe	Legal obligation (Article 6(1)(c)) - KYC and AML; performance of contract (Article 6(1)(b))
Crest standing of a Store	Order, dispute, refund, chargeback, payout and review records of the Store, its followers and saves, its listings' moderation flags, its enforcement actions and its verification status, within the 180-day window	Legitimate interest (Article 6(1)(f)) - a published, conduct-only trust standing for buyers and sellers
The buyer record (in good standing or not, read by a Store at checkout or booking)	Purchases completed, disputes and their outcome, reviews on completed purchases, and identity verification status, over the rolling 180-day window; older facts fall out	Legitimate interest (Article 6(1)(f)) - a fair marketplace, balanced by a private default and a right to review by a person
Legal compliance	Any data required by law	Legal obligation (Article 6(1)(c))

4. AI and your data

In brief: AI features use Claude, from our AI partner, Anthropic. Your Content is never used to train models. Retention is governed by our data processing agreement with Anthropic.

Trepup ranks feed recommendations on its own infrastructure (behaviour-based, not interest-selection) and personalises search the same way (basic on Free, personalised on Pro and Premium). It uses AI for caption generation (every tone, on every plan), AI Content Assist wherever an Actor writes (every plan, Members included, metered by the action), and Store review summaries (AI summaries of a Store's reviews, labelled, using Anthropic's Claude API).

For example, if you follow ceramic studios and save pottery posts, your feed learns to show you more ceramics - learned from behaviour, never from an interests questionnaire.

Trepup is an AI-first platform and the Claude API is its single model layer. For AI features powered by Anthropic's Claude API - caption generation, AI Content Assist, Trep, the AI that runs your Trepup, feed explanations, moderation screening, Store review summaries, and Crest statements of reasons and appeal support - your Content is sent to Anthropic for processing at the time the feature runs. Your Content is never used to train Anthropic's models. This is contractually guaranteed under our data processing agreement with Anthropic, which also governs retention.

Feed recommendations use an on-platform algorithm that analyses your interactions (views, likes, follows, saves, boosts) to surface relevant Content. This processing happens on Trepup's infrastructure and does not involve third-party AI providers.

The training commitment

Nothing you make on Trepup is used to train any AI model - not ours, not Anthropic's, not any third party's. This applies to everything you create or upload: posts, images, videos and audio, listings, product and service data, messages, reviews, your customer list, and your numbers. It applies at launch and permanently, to every model we use today and any model we may use in the future.

Two mechanisms back this commitment. First, our data processing agreement with Anthropic contractually excludes Content submitted through the Claude API from model training. Second, Trepup itself trains no models on your Content or personal data: feed recommendations and search ranking are computed by on-platform scoring of interaction signals, which personalises what you see without training a model on what you make.

This commitment can only be strengthened, never weakened. Any change to it would be a material change under Changes to this Policy, with notice before taking effect.

Automated decision-making

Trepup uses automated processing for Content recommendations, AI-generated captions, AI Content Assist, and Store review summaries. These features do not produce legal or similarly significant effects as defined by GDPR Article 22; the one automated decision that does - a Store's Crest standing - is described below. You may contact privacy@trepup.com to request a review by a person of any automated decision. Trepup's Content moderation data processing is subject to transparency requirements under the EU Digital Services Act (Regulation 2022/2065). Details on moderation practices and transparency reporting are in the Acceptable use policy.

5. Payment data

In brief: Your card data never touches our servers. Stripe handles everything. We see only a token.

All payment processing is handled by Stripe (Stripe Payments Europe, Limited, with Stripe, LLC in the United States; stripe.com). When you pay on Trepup - for a paid plan, Seats, extra Stores, Boost, metered intelligence, or a purchase from a Store - your card number, expiry date, and CVV are entered into a Stripe-hosted iframe that runs on stripe.com. This card data is transmitted directly from your browser to Stripe's servers. It never enters, transits, or is stored on any Trepup system. If you pay with a method that has its own provider - PayPal, Klarna, Billie or a bank - that provider processes your details as its own controller, under its own terms.

Payment methods - cards and the local methods Stripe presents for your country - are processed by Stripe under the payment-processing purpose (see How we use your data); Trepup receives the outcome and the currency of charge, never the credential.

Trepup receives and stores only: a Stripe payment method token (a reference ID, not card data), your Stripe customer ID, subscription status, the outcome and currency of each payment, and billing events (invoice paid, invoice failed, subscription updated, subscription cancelled). These records are stored in the billing schema of our database in eu-central-1 (Frankfurt, Germany).

This architecture places Trepup in the PCI DSS SAQ A validation category. Stripe is a PCI DSS Level 1 certified service provider - the highest level of certification in the payment card industry.

6. Who we share data with

In brief: Five sub-processors - our AI partner, Anthropic; our hosting partner, AWS; our network partner, Cloudflare; our code host, GitHub; and our payment partner, Stripe. No data sales. No advertising partners. DPAs with every provider. 30-day notice before adding a new one.

Bot defence at sign-up and sign-in. The email form and the create-account form carry Cloudflare Turnstile, an invisible check that tells a person from an automated script. In the ordinary case it shows nothing and asks nothing of you. It reads signals your browser already sends - IP address, request headers, and how the form is interacted with - and only a request that looks automated is shown a short challenge, which is Cloudflare's own and not designed by Trepup. Turnstile does not identify you, does not follow you to other sites, and is used for no purpose other than deciding whether a request is a person. Cloudflare, Inc. processes those signals on our behalf as a sub-processor, under its data processing terms, which are in the register at trepup.com/legal/trust. We rely on legitimate interest (Article 6(1)(f)) for this check: keeping the Platform free of automated abuse.

The Crest certificate. A Store may present its standing outside Trepup as a signed certificate. The certificate carries the Store's standing, score and band and its identifiers only; it never carries any buyer's personal data.

We do not sell your personal data. We do not share your personal data with advertisers, and Trepup uses no audience-matching partner. We share data only with the service providers listed below, and only to the extent necessary for each provider's function.

Recipient	What is shared	Why	Location
Anthropic, PBC	Content submitted to AI features (see AI and your data)	AI processing. Never used to train models. Retention per the Anthropic DPA.	United States (SCCs in place)
Amazon Web Services (AWS)	All Platform data (encrypted at rest AES-256 and in transit TLS 1.2+)	Hosting for the whole Platform, for every country. eu-central-1 (Frankfurt) serves the world; eu-west-3 (Paris) is disaster recovery.	EU only (Frankfurt, Paris)
Cloudflare, Inc.	Request signals on the sign-up and sign-in forms - IP address, request headers, interaction timing; and, as the photos and videos people post are delivered, each request's IP address and headers, with the file matched against known child sexual abuse material; and, when a call is set up, the device's IP address, as its STUN server answers it. No Account data.	Bot defence (Cloudflare Turnstile); delivering media and detecting known child sexual abuse material; finding a call's direct route (STUN).	United States (Data Privacy Framework and SCCs)
GitHub (Microsoft)	Source code and CI/CD. Developer account identifiers in commit metadata only. No end-user personal data.	Development and deployment.	United States (Data Privacy Framework and SCCs)
Stripe Payments Europe, Limited; Stripe, LLC	Payment token, customer and transaction IDs, subscription events, sellers' payout details; identity verification data, including identity documents and any selfie match, collected by Stripe	Payment processing and identity verification. PCI DSS Level 1.	Ireland and United States (Data Privacy Framework and SCCs)

We will notify you at least 30 days before adding a new sub-processor. The current sub-processor list, data processing agreements, and transfer impact assessments are published at trepup.com/legal/trust. This page is updated within 24 hours of any change to our sub-processor list. If you object to a new sub-processor, you may terminate your Account and we will delete your data.

Every sub-processor listed above processes personal data under its own data processing terms, which apply to our use of its service: they bind it to process your data only on our instructions, to secure it, to notify us of breaches, to delete it when the service ends, and to submit to audit. For each, we have performed a transfer impact assessment. The terms in force, the legal basis for any transfer, and each assessment are published at trepup.com/legal/trust.

We may disclose personal data if required by law, regulation, legal process, or enforceable governmental request. We will notify you of such requests unless legally prohibited from doing so. Government data access requests are logged separately. The number and type of requests received,

the number complied with, and the number where notification was legally prohibited are reported in our annual transparency reports.

For example, nothing ever reaches the advertising exception without action from you: a Premium Store Owner must switch the opt-in on, and switching it off stops the sharing.

7. Where your data lives

In brief: Frankfurt, Germany (EU), serving every country. Disaster recovery in Paris. No data leaves the EU except to Anthropic, Cloudflare, GitHub, and Stripe (US, with safeguards in place).

All personal data and operational data is stored in the European Union. Our primary data centre is currently eu-central-1 (Frankfurt, Germany), with disaster recovery currently in eu-west-3 (Paris, France); both are always within the European Union. Cross-region replication is restricted to the Frankfurt-Paris pair. No data is replicated to regions outside the EU.

Where we transfer data to sub-processors outside the EU (Anthropic, Cloudflare, GitHub, and Stripe in the United States), we rely on appropriate safeguards under Chapter V GDPR. For Anthropic we rely on Standard Contractual Clauses (SCCs) approved by the European Commission (Decision 2021/914), supplemented by a transfer impact assessment. Cloudflare, GitHub and Stripe are self-certified under the EU-US Data Privacy Framework and the Swiss-US Data Privacy Framework, with SCCs as a fallback. For transfers from Switzerland, the SCCs are supplemented with Swiss-specific amendments recognised by the FDPIC. If a safeguard we rely on is invalidated or replaced, we transition the affected transfers to a lawful successor safeguard and update the register at trepup.com/legal/trust within 30 days.

For transfers from the United Kingdom, we rely on the International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs approved by the UK Secretary of State.

8. Cookies and session management

In brief: One essential cookie. No tracking. No analytics cookies. Stripe's and Cloudflare's frames may set their own, as the Cookie policy describes. No consent banner needed because we use only strictly necessary cookies.

Trepup uses essential cookies for authentication and session management only. We do not use tracking cookies, advertising cookies, or analytics cookies from third parties. Because we use only strictly necessary cookies (as defined by Article 5(3) of the ePrivacy Directive), no cookie consent banner is required. You will not see a cookie pop-up on Trepup. If we ever add non-essential cookies in the future, we will implement a consent mechanism before doing so and update this Policy.

Cookie	Purpose	Duration	Type
trepup_refresh	Refresh token for session continuity	7 days	httpOnly, secure, sameSite=lax

Access tokens (15-minute expiry) are held in application memory only. They are never stored in cookies, localStorage, or sessionStorage. When you close the browser tab, the access token is gone. A new access token is obtained from the refresh token when you return.

Trepup does not use any of the following: Google Analytics, Facebook Pixel, advertising network cookies, fingerprinting scripts, or any other tracking technology. The one bot-defence check on the sign-up and sign-in forms, Cloudflare Turnstile, reads request signals to tell a person from a script; it

does not identify or track you (see Who we share data with). We do not participate in real-time bidding or ad exchanges.

9. How we protect your data

In brief: Passwordless. AES-256 at rest. TLS 1.2+ in transit. Opaque session tokens. Private VPC. No SSH to containers.

Trepup is passwordless by design. There are no passwords to steal, no password hashes to crack, and no password reset flows to exploit. Authentication uses three methods: email magic links, Google OAuth, and Sign in with Apple.

Encryption at rest

AES-256 on all data stored in Amazon RDS (PostgreSQL 16) and Amazon S3. Encryption keys are managed by AWS Key Management Service (KMS). We do not manage our own encryption keys.

Encryption in transit

TLS 1.2 or higher on all connections. HSTS enforced. No plaintext HTTP endpoints.

Session security

Session tokens are opaque random bytes (crypto.randomBytes(32)), SHA-256 hashed before storage. The auth-api service is the sole token authority. Access tokens expire after 15 minutes. Refresh tokens expire after 7 days and are stored in httpOnly, secure, sameSite=lax cookies only.

Infrastructure security

Private VPC with no public subnets for application services. Security groups restricted to minimum required ports. IAM roles scoped with least privilege. AWS CloudTrail enabled for audit logging. No SSH access to production containers (ECS Fargate).

10. Data breach notification

In brief: We notify the regulator within 72 hours and you by email and in-app banner if the breach poses high risk.

If the breach is likely to result in a high risk to your rights and freedoms, we will notify you directly without undue delay, as required by GDPR Article 34. Notification will be sent to your registered email address and displayed as an in-app banner when you next open Trepup.

Notification will include: the nature of the breach, the categories and approximate number of individuals affected, the likely consequences, and the measures taken or proposed to address the breach. We will also notify the Swiss FDPIC as required under the FADP.

11. How long we keep your data

In brief: Account data until you delete. Billing records 10 years (Swiss law). Logs 90 days. Tokens expire automatically.

Data type	Retention period	Basis
Account data	Until you delete your Account + 30-day grace period	Contract performance
Content you create (posts, reviews, messages)	Until you delete the Content or your Account	Contract performance
Payment and billing records	10 years from the end of the fiscal year (Swiss Code of Obligations Article 958f)	Legal obligation
Session tokens (access)	15 minutes	Automatic expiry
Session tokens (refresh)	7 days	Automatic expiry
Magic links	15 minutes	Automatic expiry
Server logs (IP, device)	90 days rolling	Legitimate interest (security)
Anonymised analytics	Indefinite (not personal data after anonymisation)	N/A

When you delete your Account, we begin a 30-day grace period during which you can reactivate. After 30 days, we permanently delete your personal data from all active systems. Backup retention follows the backup schedule (daily backups retained for 7 days, weekly backups retained for 4 weeks). Data in backups is overwritten on schedule and is not actively processed.

We review our data retention schedule annually. If we determine that data is no longer necessary for the purpose for which it was collected, we delete it. The first review was completed before this Policy took effect.

12. Your rights

In brief: Access, rectification, erasure, portability, restriction, objection, consent withdrawal. Immediate acknowledgement, 7-day completion. Free of charge.

You have the following rights over your personal data. These rights apply to every Trepup user regardless of location. We apply the GDPR standard globally.

Right of access (GDPR Article 15)

You can request a copy of all personal data we hold about you. We will provide this in a structured, commonly used, machine-readable format (JSON).

For example, asking for your data is one request: the export arrives as a machine-readable file, acknowledged immediately and completed within 7 days, free of charge.

Right to rectification (GDPR Article 16)

You can update your personal data at any time through your profile settings. If you need to correct data you cannot edit yourself, contact privacy@trepup.com.

Right to erasure (GDPR Article 17)

You can delete your Account at any time through your Account settings (currently Settings > Account management > Delete account). This triggers a 30-day grace period followed by permanent deletion of your profile, Content, messages, orders, reviews, and all associated metadata from active systems. Your handle is released and becomes available for new Accounts. Backup copies are overwritten on the standard backup rotation schedule (daily backups: 7 days, weekly backups: 4 weeks). You can also request erasure by contacting privacy@trepup.com.

Right to data portability (GDPR Article 20)

You can export all your data at any time through your Account settings (currently Settings > Account management > Download your data). The export is delivered as a JSON file containing your profile information, posts and captions, products and services, reviews you have written, messages, order history, follows, saves, and boost history. Media files (photos, videos, and audio) are included as direct download links valid for 7 days.

Right to restriction of processing (GDPR Article 18)

You can request that we restrict processing of your data in certain circumstances (for example, while we verify accuracy of contested data). Contact privacy@trepup.com.

Right to object (GDPR Article 21)

You can object to processing based on legitimate interest (feed personalisation, promotions matched to your country, age and gender, abuse prevention). We will stop processing unless we demonstrate compelling legitimate grounds - except for promotions, where your objection always stands: it is a switch in Settings and takes effect at once. Contact privacy@trepup.com.

Right to withdraw consent

Where processing is based on consent (personalised promotions), you may withdraw consent at any time in Settings. Withdrawal does not affect the lawfulness of processing before withdrawal.

Response times

Every data subject request receives an immediate automated acknowledgement. We complete requests within 7 working days. For complex requests, we may extend the completion time to 30 days with notice. All requests are free of charge unless manifestly unfounded or excessive.

Automated decisions and your rights

Trepup makes one decision by automated means with a significant effect: a Store's Crest standing, computed each day from the Store's own record, applies automatically what the Commerce policy sets out - at Faded, in-thread checkout is off, and a Dark Store cannot be found and takes no new orders. A buyer's two-state record is only a signal, in good standing or not; the decision to decline a buyer is the Store's. You may ask for a review by a person of either - a Store's standing, or a Store's decision about you - within 30 days through the trust page; a person answers within 5 working days. Your record's inputs are visible to you in settings at any time.

Supervisory authority

You have the right to lodge a complaint with a supervisory authority. For Swiss residents, the relevant authority is the Federal Data Protection and Information Commissioner (FDPIC) at edoeb.admin.ch. For EU residents, you may contact the supervisory authority in your member state of residence. For UK residents, the relevant authority is the Information Commissioner's Office (ICO) at ico.org.uk.

Do Not Track

Trepup does not track users across third-party websites and therefore does not respond to Do Not Track (DNT) browser signals. We do not need to - we do not engage in the cross-site tracking that DNT is designed to prevent.

Global Privacy Control

Trepup recognises the Global Privacy Control (GPC) signal. When your browser sends a GPC signal, we treat it as a valid opt-out request under the CCPA, CPRA, and any US state law that requires recognition of opt-out preference signals. In practice, because Trepup does not sell personal information, does not share personal information for cross-context behavioural advertising, and does not engage in cross-site tracking, there is no data sale or sharing activity to cease. The GPC signal is acknowledged and logged, and no further action is required because the activity it is designed to prevent does not occur on Trepup.

Marketing communications

You can opt out of marketing emails at any time by clicking the unsubscribe link in any marketing email or through your notification settings. Transactional emails (order confirmations, security alerts, Account changes) are not affected by this preference.

13. California residents

In brief: CCPA/CPRA rights. We do not sell personal information. We do not share for targeted advertising.

If you are a California resident, the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA) provides you with additional rights. This section supplements the rest of this Policy.

Categories of personal information collected

Identifiers (name, email, handle, and a Store's contact phone), internet or electronic network activity (usage data, IP address), commercial information (purchase history, subscription status), and inferences drawn from these categories (feed recommendations).

Sale of personal information

We do not sell your personal information as defined by the CCPA. We have never sold personal information.

Sharing for targeted advertising

We do not share your personal information for cross-context behavioural advertising as defined by the CPRA.

Your CCPA rights

Right to know what personal information is collected, right to delete, right to correct, right to opt out of the sale of personal information (not applicable - we do not sell), and right to non-discrimination for exercising your rights.

To exercise your CCPA rights, contact privacy@trepup.com. We will verify your identity before processing any request. You may designate an authorised agent to make a request on your behalf.

14. United Kingdom residents

In brief: UK GDPR applies. Transfers via adequacy decisions or UK SCCs. Complaints to the ICO.

If you are a resident of the United Kingdom, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 apply to the processing of your personal data. This section supplements the rest of this Policy.

Trepup.com AG is the data controller. We do not have a UK representative appointed under Article 27 of the UK GDPR at this time. If one is appointed, the details will be published on trepup.com/legal/trust.

Where we transfer your personal data outside the UK, we rely on adequacy decisions (for Switzerland and the EU) or the International Data Transfer Agreement (IDTA) or UK Addendum to the EU SCCs approved by the UK Secretary of State.

You have the right to lodge a complaint with the Information Commissioner's Office (ICO) at ico.org.uk.

15. Global coverage

In brief: GDPR-level rights for every user on earth. 23 jurisdictions in one reference table. 90-day commitment for new laws.

Trepup is available in every country and territory where internet access exists. We apply the same data protection standard to every user regardless of location. That standard is the GDPR - the most protective general data protection regime in force. If your country has a privacy law that grants you specific rights, those rights are honoured in addition to the GDPR baseline. You do not receive a lesser standard because your country has a weaker privacy law or no privacy law at all.

The rights under Your rights (access, rectification, erasure, portability, restriction, objection, consent withdrawal) apply to every user on the Platform. The response SLA (immediate acknowledgement, 7-day completion) applies globally. The data export format (JSON) applies globally. The sub-processor list and 30-day change notice apply globally.

Jurisdiction details

The following table summarises the rights, complaint authority, and authority URL for each jurisdiction. If your jurisdiction is not listed, the full set of rights under Your rights applies to you.

Jurisdiction	Law	Rights	Authority
Argentina	PDPL (Law 25.326)	Access, rectify, suppress, object	EU adequacy recognised
Australia	Privacy Act 1988 / APPs	Access (APP 12), correct (APP 13)	OAIC (oaic.gov.au)
Brazil	LGPD (Law 13.709/2018)	Access, correction, anonymisation, portability, consent revocation	ANPD (gov.br/anpd)
Canada	PIPEDA / Quebec Law 25	Access, correct, withdraw consent	Privacy Commissioner (priv.gc.ca)
China	PIPL	Know, restrict, access, portability, correction, deletion	CAC (SCCs filed)
India	DPDPA 2023	Access, correction, erasure, grievance redressal, nomination	Data Protection Board
Indonesia	PDP Law (Law 27/2022)	Access, correct, delete, withdraw consent, object to profiling	National authority
Israel	Protection of Privacy Law 5741-1981	Review, correct, delete	EU adequacy recognised
Japan	APPI	Disclosure, correction, cessation of use, deletion	PPC (ppc.go.jp). EU adequacy.
Kenya	Data Protection Act 2019	Be informed, access, object, correct, delete	ODPC (odpc.go.ke)
Malaysia	PDPA 2010	Access, correct, withdraw consent	PDP (pdp.gov.my)
Mexico	LFPDPPP	ARCO: access, rectification, cancellation, opposition	INAI (home.inai.org.mx)
New Zealand	Privacy Act 2020	Access, correct	Privacy Commissioner (privacy.org.nz). EU adequacy.
Nigeria	NDPR 2019 / NDP Act 2023	Be informed, access, rectify, erase, portability	NDPC (ndpc.gov.ng)
Philippines	DPA 2012 (RA 10173)	Be informed, access, object, erase, rectify, portability, damages	NPC (privacy.gov.ph)
Saudi Arabia	PDPL (Royal Decree M/19)	Be informed, access, correct, destroy, withdraw consent	SDAIA
Singapore	PDPA 2012	Access, correct, withdraw consent	PDPC (pdpc.gov.sg)

Jurisdiction	Law	Rights	Authority
South Africa	POPIA	Be notified, access, correct, delete, object	Information Regulator (inforegulator.org.za)
South Korea	PIPA	Access, correct, delete, suspend processing	PIPC (pipc.go.kr). EU adequacy.
Thailand	PDPA B.E. 2562	Access, portability, object, erase, restrict, rectify, withdraw consent	PDPC
Turkey	KVKK (Law 6698)	Learn, request info, learn purpose, know transfers, rectify, erase	KVKK (kvkk.gov.tr)
UAE	Federal Decree-Law No. 45/2021	Access, correct, cease processing, erase, portability	UAE Data Office
United States (non-CA)	VCDPA, CPA, CTDPA, UCPA, TDPSA, OCPA, MTCDPA, others	Know, delete, correct, opt out of sale	Contact privacy@trepup.com

We apply the GDPR standard globally. If your country enacts new data protection legislation after this Policy is published, we will update this section within 90 days of the law taking effect. All updates are logged on our legal updates page at trepup.com/legal/updates.

16. Age requirement

In brief: You must be 18 or older. We delete Accounts belonging to minors on notice.

Trepup is not intended for anyone under 18 years of age. We do not knowingly collect personal data from minors. If you believe someone under 18 has created an Account, contact privacy@trepup.com and we will delete the Account and associated data promptly.

17. Definitions

In brief: Every acronym used in this Policy, explained in plain language.

The following terms are used throughout this Policy. Every acronym is expanded here so you do not need to look it up elsewhere.

Term	Meaning
AES-256	Advanced Encryption Standard with a 256-bit key. The encryption method used to protect data stored on disk.
ANPD	Autoridade Nacional de Protecao de Dados. Brazil's national data protection authority.
APPI	Act on the Protection of Personal Information. Japan's data protection law.
APPs	Australian Privacy Principles. The 13 principles under Australia's Privacy Act 1988 governing the handling of personal information.
CCPA	California Consumer Privacy Act. California's consumer data privacy law (Cal. Civ. Code 1798.100 et seq.).
CI/CD	Continuous Integration / Continuous Deployment. Automated software build and release pipelines.

Term	Meaning
CPRA	California Privacy Rights Act. Amendments to the CCPA effective 1 January 2023, expanding consumer rights.
CVV	Card Verification Value. The 3-digit security code on the back of a payment card.
DNT	Do Not Track. A browser setting that signals a preference not to be tracked across websites.
DPDPA	Digital Personal Data Protection Act 2023. India's data protection law.
DSA	Digital Services Act (Regulation 2022/2065). The EU regulation governing transparency and accountability for digital platforms, including Content moderation reporting.
ECS	Elastic Container Service (AWS). The service that runs Trepup application containers.
FADP	Swiss Federal Act on Data Protection (Bundesgesetz ueber den Datenschutz, SR 235.1). Switzerland's national data protection law, revised 1 September 2023.
FDPIC	Federal Data Protection and Information Commissioner. Switzerland's data protection supervisory authority.
GDPR	General Data Protection Regulation (EU) 2016/679. The European Union's data protection law.
HSTS	HTTP Strict Transport Security. A web security mechanism that forces browsers to use HTTPS.
httpOnly	A cookie attribute that prevents JavaScript from reading the cookie.
ICO	Information Commissioner's Office. The United Kingdom's data protection supervisory authority.
IDTA	International Data Transfer Agreement. The UK's approved mechanism for transfers of personal data outside the UK.
KVKK	Kisisel Verileri Koruma Kurumu. Turkey's Personal Data Protection Authority.
LFPDPPP	Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares. Mexico's federal data protection law for private parties.
LGPD	Lei Geral de Protecao de Dados (Law 13.709/2018). Brazil's general data protection law.
NDPR	Nigeria Data Protection Regulation 2019. Nigeria's data protection framework.
nDSG	Revised Swiss Federal Act on Data Protection (neues Datenschutzgesetz), effective 1 September 2023. Same as FADP.
PCI DSS	Payment Card Industry Data Security Standard. The information security standard for organisations that handle payment card data.
PDPA	Personal Data Protection Act. Data protection law in Singapore (2012) and Thailand (B.E. 2562).
PDPL	Personal Data Protection Law. Data protection law in Argentina (Law 25.326) and Saudi Arabia (Royal Decree M/19).
PIPA	Personal Information Protection Act. South Korea's data protection law.

Term	Meaning
PIPEDA	Personal Information Protection and Electronic Documents Act. Canada's federal privacy law.
PIPL	Personal Information Protection Law. China's data protection law.
POPIA	Protection of Personal Information Act. South Africa's data protection law.
SAQ A	Self-Assessment Questionnaire A. A PCI DSS validation type for merchants that fully outsource card data handling.
SCCs	Standard Contractual Clauses. EU-approved contractual mechanism for transferring personal data outside the EEA.
TLS	Transport Layer Security. The cryptographic protocol that secures data in transit between your browser and our servers.

18. Changes to this Policy

In brief: We give you 30 days notice before material changes, through the Platform and by email. English prevails. All changes logged at trepup.com/legal/updates.

We may update this Policy from time to time. When we make material changes, we will notify you through the Platform and by email at least 30 days before the change takes effect. Non-material changes (clarifications, formatting, spelling corrections) take effect immediately.

All changes are logged on our legal updates page at trepup.com/legal/updates with a description of what changed, why, and the effective date.

This Policy is published in English. If this Policy is translated into any other language, the English-language version prevails in the event of any conflict or ambiguity.

19. Contact

In brief: Four email addresses - support, privacy, legal, security. Replies are typically immediate.

For any privacy-related questions, data subject requests, or complaints, contact us at:

Trepup.com AG

Attn: Legal

Poststrasse 30, CH-6300 Zug, Switzerland

CHE-350.031.599

General support: support@trepup.com

Privacy inquiries: privacy@trepup.com

Legal inquiries: legal@trepup.com

Security reports: security@trepup.com

Trep answers at once. A person is always reachable at these addresses, and you can always have a complaint or appeal decided by a person.

If you are not satisfied with our response, you have the right to lodge a complaint with the relevant supervisory authority as described under Your rights.

This Policy is effective 1 December 2026.