

SPONTLR

Privacy Policy

Effective Date: April 16, 2026 · Version 1.1

Spontlr Inc. · 131 Continental Drive, Suite 305, Newark, Delaware 19713, USA

The Short Version

Plain English summary. The full policy below is the legally binding version.

- We collect only what we need to run Spontlr — nothing extra.
- We never sell your data. Not to advertisers, not to anyone.
- We do not track your behavior. We don't watch what you tap, scroll, or look at.
- Your location is used in the moment to show nearby content — we don't store or log your movements.
- Your data lives on servers in Frankfurt, Germany — inside the European Union.
- You have full rights: access, correct, export, or delete your data anytime.
- We comply with both EU law (GDPR) and US law.
- Questions? We're real people: privacy@spontlr.com

1. Who We Are

Spontlr is a verified lifestyle community app. We connect real, ID-verified people with each other and with local businesses — so you can explore your city, earn real rewards, and be part of something genuine.

We are not a social media app. We don't sell advertising. We don't profile you. We exist to help you do life — not to monetise your attention.

Company:	Spontlr Inc.
Registered address:	131 Continental Drive, Suite 305, Newark, Delaware 19713, USA
Data stored in:	Frankfurt, Germany (European Union)
General contact:	hello@spontlr.com
Privacy contact:	privacy@spontlr.com
Data Protection:	dpo@spontlr.com

Spontlr Inc. is the data controller for all personal data described in this policy. This means we are responsible for how your data is used and protected.

2. What Data We Collect

We collect the minimum we need to make Spontlr work safely. Here is everything, explained plainly.

Data you give us directly

- Full name and date of birth — required to verify your identity and confirm you are 16 or older
- Email address and password — to create and access your account
- Profile photo, bio, location (city), job title, and any other profile fields you choose to fill in
- Posts, photos, and content you share on Spontlr — visible to other verified members
- Messages you send to other members — private and encrypted in transit
- Government-issued ID — submitted once for identity verification. Not stored by Spontlr after verification is complete.

Data we collect automatically

- Your device type and operating system — for technical compatibility and security
- IP address — for security, fraud prevention, and detecting suspicious activity
- Your location — only when you open the app and only if you grant permission (explained in Section 5)

What we deliberately do NOT collect

Spontlr does not track your behavior inside the app. We do not log which screens you visit, which posts you scroll past, which profiles you view, how long you use the app, or what you tap. We do not build behavioral profiles. We do not use your in-app activity to personalise what you see or to sell advertising. This is a deliberate choice — it is core to what Spontlr stands for.

3. Why We Use Your Data

Every piece of data we collect has a specific reason. Here they are:

To run Spontlr

- Create and manage your account
- Verify your identity so the community stays real, safe, and fraud-free
- Show you content, people, and businesses near your current location
- Enable you to post, comment, and connect with other verified members
- Process your subscription payments and manage your rewards points balance

To keep Spontlr safe

- Detect and prevent fake accounts, bots, and abuse
- Enforce our Community Standards and respond to reports

- Protect against fraud, account takeovers, and unauthorised access
- Ensure members who lie about their age are identified and removed

To communicate with you

- Send important account and security notifications — you cannot opt out of these as they keep your account safe
- Notify you about activity relevant to your posts or connections
- Occasional Spontlr updates — you can opt out of non-essential messages anytime in Settings

4. Our Legal Basis for Using Your Data (EU / GDPR)

If you are in the European Union or EEA, data protection law requires us to have a documented legal reason for each use of your data. Here is ours:

- Contract performance — we process your data because you signed up and we need it to deliver the service you agreed to
- Legitimate interests — keeping the platform safe, preventing fraud, and fixing technical issues. We always balance this against your rights.
- Legal obligation — where the law requires us to retain certain records (for example, payment records for tax purposes)
- Consent — where we ask for your explicit permission first, such as for location access. You can withdraw consent at any time in your device settings.

5. Your Location Data — How It Really Works

Location is central to what Spontlr does. But how we use it is very different from most apps. Here is the honest explanation:

What actually happens when you open the app

When you open Spontlr, your device shares your current coordinates with our system. Those coordinates are passed into a database query that calculates which posts, people, and businesses are nearest to you — and returns them sorted by distance. That is it. The query runs, the results come back, and your coordinates are not stored, logged, or recorded anywhere.

What we do NOT do with your location

- We do not store a history of where you have been
- We do not log which businesses or posts you looked at near a specific location
- We do not build a movement profile or location timeline
- We do not use your location history to personalise what you see in the future
- We do not share your precise location with other members — content only shows a general area
- We do not sell location data to anyone, ever

Location attached to your posts

When you create a post, you choose whether to attach a location to it. If you do, that location is stored as part of the post so it appears in the nearby feed for other members. You are always in control of whether your posts are location-tagged.

Think of it this way: we use your location like a compass, not a tracking device. It points you toward what is nearby right now. Then you decide what to explore. We don't watch what you choose.

- Location access requires your permission — grant or revoke it anytime in your phone Settings
- If you do not grant location permission, the app still works — you just won't see distance-sorted results

6. Who We Share Your Data With

We do not sell your data. Full stop. We share it only in the following situations:

Our infrastructure provider

- Supabase — our database, authentication system, and file storage. All data is stored on Supabase infrastructure hosted in Frankfurt, Germany (EU). Supabase is contractually required to protect your data and may not use it for any other purpose.

Payment processing

- Stripe — processes subscription payments securely. We never see or store your card number. Stripe is PCI-DSS Level 1 certified.
- RevenueCat — manages in-app subscription states on iOS. They receive purchase confirmation, not your payment details.
- Apple App Store / Google Play — handle in-app purchase transactions where applicable.

Other verified members

- Your public profile, display name, profile photo, and posts are visible to other verified members
- Your precise location is never shared with other members

Legal requirements

- We may disclose data if required by a valid court order or applicable law
- We may share data to protect the safety of our members or the public in an emergency
- We will notify you whenever legally possible if your data is requested

Business transfers

- If Spontlr is acquired or merges with another company, your data may transfer to the new entity. We will notify you before this happens and you will have the right to delete your account.

7. Where Your Data Is Stored

Your data is stored on servers located in Frankfurt, Germany — inside the European Union. This is where Spontlr's infrastructure is hosted.

Spontlr Inc. is incorporated in Delaware, USA, but we chose EU-based infrastructure intentionally to give our European members the strongest possible data protection by default.

When data does cross borders

Some of our service providers (such as Stripe and RevenueCat) process data in the United States. When this happens, we ensure it is protected by:

- Standard Contractual Clauses (SCCs) — legal agreements approved by the European Commission that require US-based providers to protect EU data to EU standards
- Only working with providers who meet or exceed GDPR requirements

EU Representative: As a US-incorporated company serving EU users, we are in the process of formally appointing an EU representative under GDPR Article 27. In the meantime, all EU privacy inquiries are handled directly at dpo@spontlr.com.

8. How Long We Keep Your Data

We keep your data only as long as necessary. Here is the breakdown:

- Account data — kept while your account is active, plus 30 days after deletion in case you change your mind
- Your posts and content — deleted immediately when you remove them, or when you delete your account
- Private messages — deleted when both parties delete the conversation, or when accounts are deleted
- Payment records — retained for 7 years as required by US and EU tax law
- Government ID — deleted immediately after identity verification is complete. We do not keep a copy.
- IP address logs — retained for 90 days for security purposes, then permanently deleted

When you delete your account, permanent deletion begins within 30 days. Some data may persist in anonymised, aggregated form — it cannot be traced back to you.

9. Your Rights

You are in control of your data. Here is what you can do:

Your Right	What it means in practice
Access	See all the data we hold about you
Correct	Fix anything that is wrong or outdated
Delete	Ask us to delete your account and all your data
Export	Get a copy of your data in a readable format
Object	Object to certain uses of your data

Restrict	Ask us to pause processing your data
Withdraw consent	Change your mind on anything you previously agreed to
Complain	File a complaint with a data protection authority

To exercise any of these rights, email privacy@spontlr.com. We will respond within 30 days (usually much sooner).

If you are in the EU, you also have the right to file a complaint with your local data protection authority. In Poland: UODO (uodo.gov.pl). In Germany: BfDI (bfdi.bund.de).

10. How We Protect Your Data

- All data is encrypted in transit (TLS) and encrypted at rest on our servers
- Our database uses Row Level Security — each member can only access their own data, enforced at database level
- Access to member data by Spontlr staff is strictly limited and logged
- Payments are handled by Stripe (PCI-DSS Level 1 certified) — we never see or store payment card details
- Government ID documents are processed and immediately discarded — not retained

No system is 100% secure. If we ever experience a data breach that affects you, we will notify you and the relevant authorities within the timeframes required by law — within 72 hours to EU regulators, and promptly to affected members.

11. Age Policy — 16 and Over Only

Spontlr is for people aged 16 and over. Students and young adults are welcome — but no one under 16 may use the app.

We enforce this through mandatory ID verification during signup. Your date of birth must match your government-issued ID. If they do not match, the account is rejected.

If we discover that a member is under 16 — through verification, a report, or any other means — we will permanently delete their account and all associated data immediately.

If you believe someone under 16 has an account, please report it to privacy@spontlr.com. We take this seriously and will act quickly.

12. California Residents (CCPA / CPRA)

If you are a California resident, you have additional rights under California privacy law:

- Right to know what personal information we collect, use, and share
- Right to delete your personal information
- Right to correct inaccurate personal information
- Right to opt out of the sale or sharing of your personal information — we do not sell or share your data for advertising

- Right to limit use of sensitive personal information
- Right to non-discrimination for exercising any of these rights

To make a California privacy request, email privacy@spontlr.com with the subject line 'California Privacy Request'. We will respond within 45 days.

13. Changes to This Policy

We may update this policy as Spontlr grows or as laws change. When we do:

- The Effective Date at the top of this document will be updated
- For significant changes affecting your rights, we will notify you in the app and by email at least 14 days before the change takes effect
- The current version is always available in the app under Settings > Privacy Policy

If you continue using Spontlr after an update, this means you accept the revised policy. If you disagree with a change, you can delete your account at any time.

14. Contact Us

Privacy questions, data requests, or anything else — we are real people and we will get back to you.

General privacy questions: privacy@spontlr.com

Data Protection Officer: dpo@spontlr.com

Post: Spontlr Inc., 131 Continental Drive, Suite 305, Newark, Delaware 19713, USA

We aim to respond within 30 days. Usually much faster.

EU supervisory authority (Poland): UODO — uodo.gov.pl

EU supervisory authority (Germany): BfDI — bfdi.bund.de

California privacy authority: CPPA — cppa.ca.gov

This Privacy Policy was prepared for Spontlr Inc. and reflects data practices as of the effective date above. It is designed to comply with GDPR (EU/EEA), CCPA/CPRA (California), and applicable US federal and state privacy laws. This document is not a substitute for independent legal advice.