

PRIVACY POLICY

Inwall Application & Website

Last Updated: April 16, 2026

Inwall Inc. | 131 Continental Dr, Newark, DE 19713 | contact@inwall.app

1. Introduction

Inwall Inc. (“Inwall,” “we,” “us,” or “our”) is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, store, and protect information about you when you use the Inwall mobile application (“App”) and website (“Website”), collectively the “Platform.”

By using the Platform, you agree to the collection and use of your information as described in this Privacy Policy. This Policy applies to all Users (individuals paid for sharing sponsored content on their social media) and Advertisers (businesses running advertising campaigns).

2. Information We Collect

2.1 Information Collected from Users

When you register and use the Platform as a User, we collect:

Account & Identity Information:

- First name and last name
- Email address and phone number
- Date of birth and gender
- Nationality, residential address, and country of residence

Identity Verification (KYC) Data:

KYC verification is administered through Stripe Identity. In connection with KYC, we and/or Stripe may collect government-issued photo identification (e.g., passport, driver’s license, or state ID) and biometric data (facial scan or selfie for identity matching). Government-issued identification and biometric data are sensitive categories of personal information, collected solely to verify your identity and comply with legal obligations. Raw identity documents are processed by Stripe Identity under Stripe’s Privacy Policy; Inwall does not retain copies on its own servers beyond what is technically necessary.

Social Media Information:

- Social media handles, usernames, and profile links
- Self-reported audience size and engagement metrics
- Self-reported content interests and audience demographics
- Data authorized through social media OAuth connections (subject to permissions you grant)

Financial Information:

- Stripe Connect account information (processed directly by Stripe)
- Payout history and earnings records
- IRS Form W-9 information (where required for tax reporting)

2.2 Information Collected from Advertisers**Business & Contact Information:**

- Company name and country of incorporation
- First name, last name, and job title of the primary point of contact
- Business email address and phone number
- Company logo and brand assets

Campaign Information:

- Advertising creatives (video and image files)
- Target audience parameters (location, gender, age range, social media popularity, and interests)
- Pay Per Share (PPS) amount and advertising budget
- Spend history and campaign performance data

2.3 Information Collected Automatically

When you use the Platform, we automatically collect: log data (access times, pages viewed, errors), device information (hardware model, operating system, unique device identifiers), IP address and approximate geographic location, and analytics data regarding how you interact with the Platform.

2.4 Information from Third Parties

We may receive information from third parties including: Stripe Identity (identity verification results and risk flags), Stripe Connect (payment processing status and fraud signals), and social media platforms (information you authorize through OAuth or API connections).

3. How We Use Your Information

We use the information we collect to:

- Create and manage your account and authenticate your identity.
- Facilitate Pay Per Share campaigns and track valid shares.
- Process payouts and payments through Stripe Connect.

- Detect, investigate, and prevent fraud, abuse, and policy violations.
- Comply with legal obligations, including tax reporting (e.g., IRS Form 1099-NEC).
- Respond to lawful requests from government authorities and law enforcement.
- Send transactional emails, payment notifications, and policy updates.
- Send promotional communications (with your consent where required).
- Match Users with relevant Campaigns based on collected data including social media audience and interests.
- Analyze Platform usage and improve features and functionality.

4. How We Share Your Information

We do not sell your personal information to third parties. We may share your information in the following limited circumstances:

4.1 Service Providers

We share information with trusted third-party service providers under confidentiality obligations, including: Stripe, Inc. (payment processing via Stripe Connect and identity verification via Stripe Identity); cloud hosting and infrastructure providers; analytics providers; and email and communication service providers.

4.2 Between Users and Advertisers

Advertisers do not receive personally identifiable information about individual Users. Advertisers receive only aggregated and anonymized Campaign performance data. Users are not provided with the personal contact details of Advertiser representatives beyond publicly displayed Campaign information.

4.3 Legal Requirements

We may disclose your information as required by law or in response to valid legal process (court order, subpoena, search warrant), or as necessary to protect the rights, property, or safety of Inwall, its users, or the public.

4.4 Business Transfers

In the event of a merger, acquisition, or sale of assets, your information may be transferred to the acquiring entity. We will provide notice of any such transfer where required by applicable law.

5. Sensitive Information

We process the following categories of sensitive personal information:

- **Government-issued identification and biometric data:** Collected solely for KYC identity verification through Stripe Identity. We do not use biometric data for any other purpose and do not sell or license biometric data to any third party.
- **Financial account information:** Collected solely for the purpose of processing payouts via Stripe Connect.
- **Social media audience data and interests:** Used solely for Campaign matching within the Platform.

6. Data Retention

We retain personal information as long as necessary to fulfill the purposes described in this Policy, or as required by law:

- Account information: retained for the duration of your account and up to 5 years following account closure.
- KYC and identity verification records: retained for the period required by applicable anti-money laundering regulations (generally a minimum of 5 years from the date of verification).
- Transaction and earnings records: retained for a minimum of 7 years for tax and audit purposes.
- Usage and log data: retained for up to 2 years.
- Campaign data: retained for the Campaign duration and up to 3 years thereafter.

Upon account deletion, we will anonymize or delete personal data no longer required for legal or operational purposes, subject to the retention periods above.

7. Data Security

We implement commercially reasonable technical, administrative, and physical safeguards to protect your information, including encryption of data in transit (TLS/SSL) and at rest, access controls limiting employee access on a need-to-know basis, regular security assessments, and use of security-certified third-party service providers.

No method of transmission over the internet is 100% secure. We cannot guarantee absolute security. In the event of a data breach affecting your rights, we will notify you as required by applicable law. If you believe your account has been compromised, contact us immediately at contact@inwall.app.

8. Cookies and Tracking Technologies

We and our service providers use cookies, web beacons, and similar technologies to maintain your session, remember preferences, analyze Platform usage, and deliver relevant content. You may configure your browser to refuse cookies, but doing so may affect Platform functionality. Where required by law, we will request your consent before setting non-essential cookies.

9. Your Privacy Rights

9.1 General Rights (All U.S. Users)

Regardless of where you reside in the United States, you have the right to:

- Access a copy of the personal information we hold about you.
- Request correction of inaccurate or incomplete information.
- Request deletion of your personal information (subject to legal retention obligations).
- Receive a copy of your data in a portable, machine-readable format where feasible.

- Opt out of promotional communications at any time via the unsubscribe link in our emails or by contacting contact@inwall.app.

9.2 California Residents – CCPA/CPRA Rights

If you are a California resident, you have additional rights under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA):

- **Right to Know:** The categories and specific pieces of personal information we collect, use, and disclose.
- **Right to Delete:** Request deletion of your personal information, subject to certain exceptions.
- **Right to Correct:** Request correction of inaccurate personal information.
- **Right to Opt-Out of Sale or Sharing:** We do not sell or share your personal information for cross-context behavioral advertising.
- **Right to Limit Use of Sensitive Personal Information:** You may limit our use of sensitive data (e.g., government ID, biometrics) to the purposes specified in this Policy.
- **Right to Non-Discrimination:** We will not discriminate against you for exercising your CCPA rights.

To exercise your CCPA rights, email contact@inwall.app with subject line “CCPA Privacy Request.” We will respond within 45 days (extendable by 45 days with notice).

9.3 How to Submit a Privacy Request

Email: contact@inwall.app with subject line “Privacy Request.” We may require identity verification before processing your request.

10. Children’s Privacy

The Platform is not directed to individuals under the age of 18. We do not knowingly collect personal information from anyone under 18. If we become aware that we have collected information from a person under 18 without verifiable parental consent, we will delete that information and terminate the associated account immediately. If you believe a person under 18 has registered, contact us at contact@inwall.app.

11. Social Media Data

When you connect a social media account to the Platform via OAuth, you authorize us to access certain data (such as public profile information, follower count, engagement metrics, and audience demographics) in accordance with the permissions you grant. We use this data solely for Campaign matching and share verification within the Platform. We do not use social media data to build behavioral advertising profiles for third parties. You may revoke our access at any time through your social media platform’s settings; however, doing so may limit your ability to properly use the Platform.

12. Links to Third-Party Sites

The Platform may contain links to third-party websites or services. This Privacy Policy does not apply to those sites. We encourage you to review the privacy policies of any third-party services you access through our Platform.

13. Changes to This Privacy Policy

We may update this Privacy Policy at any time. If we make material changes, we will notify you by email and/or a prominent notice on the Platform at least 7 days before the changes take effect. The “Last Updated” date at the top reflects the most recent revision. Your continued use of the Platform after the effective date constitutes acceptance of the updated Policy.

14. Contact Information

For questions, concerns, or privacy requests:

Inwall Inc.

131 Continental Dr,

Newark, DE 19713

Email: contact@inwall.app (subject: “Privacy Request”)

Phone: +1 (302) 307-9920

This Privacy Policy applies to both the Inwall mobile application and website.