

Privacy Policy

Effective and last updated September 4, 2026

This Privacy Policy explains how iDeep (“iDeep,” “we,” “us,” or “our”) collects, uses, shares, retains, and deletes information when you use our website and social-media content generation and publishing service (the “Service”). It applies to information processed through the Service, including information received through Meta and Instagram.

Information we collect

Account and authentication information. We collect your email address, account identifier, plan and account-creation date. We use one-time sign-in codes instead of passwords. We store a hash of each code, its expiration and verification-attempt data, not your password.

Business and brand information. We collect the company name, website, language, time zone, brand-profile answers, industry, audience, tone, content pillars, goals and other information you submit. If you provide a website, we may read and temporarily cache its public text and metadata to suggest a brand profile.

Instagram information. When you connect Instagram, we receive and store the Instagram user ID, username, professional account type, access token, token-expiration information and the permissions you grant. We also store publishing results, Instagram media identifiers and public post links. We do not request or store your Instagram password.

Content and service activity. We store prompts and topics, generated or submitted captions and images, content plans, schedules, publishing status, errors and notifications. Images generated for publishing may be hosted at a publicly accessible URL because Instagram must retrieve the image from that URL.

Device, usage and security information. We and our infrastructure and analytics providers automatically process information such as IP address, browser and device type, approximate location derived from IP, visited pages, timestamps, referring pages, request identifiers, authentication state and diagnostic or security events. We may store limited preferences and an authentication token in your browser’s local storage.

How we use information

We process information to:

- create and secure your account and authenticate you;
- build your brand profile and generate content in your chosen voice;
- schedule, publish and report on content for accounts you connect;
- operate, troubleshoot, protect and improve the Service;
- measure use and performance and prevent fraud, abuse and security incidents;
- communicate service messages and respond to support or privacy requests; and
- comply with law and enforce our Terms of Service.

Where applicable law requires a legal basis, we rely on performance of our contract, legitimate interests in operating and securing the Service, your consent where requested, and compliance with legal obligations. You may withdraw consent at any time without affecting earlier lawful processing.

How we share information

We do not sell or rent personal information. We share it only as described below:

- **Meta and Instagram:** to connect your professional Instagram account, refresh authorization, and publish the content you direct us to publish.
- **AI providers:** brand information, website-derived information, topics, prompts and content are sent to AI service providers, including Together.ai and, when configured for a generation task, OpenAI or Anthropic. We do not intentionally include your email address or Instagram access token in generation prompts.
- **Website processing:** a website URL you submit may be sent to Jina AI to retrieve and structure the public page. We may also retrieve that website directly.
- **Operations:** hosting, database, network, email and monitoring providers, including Cloudflare and Resend, process the information needed to provide their services to us.
- **Analytics:** Google Analytics processes device and usage information to help us understand Service use and performance. Browser settings or content blockers may let you limit analytics cookies or requests.
- **Legal and business events:** we may disclose information when reasonably necessary to comply with law, protect rights or safety, investigate abuse, or complete a merger, financing, acquisition or sale, subject to appropriate safeguards.

Service providers may process information only to perform services for us and under their applicable contractual and privacy obligations. We do not use customer content to train models owned by iDeep. Third-party providers process data under their own terms and our arrangements with them.

Instagram permissions and control

We use Instagram information only to provide, secure and support the connected-account and publishing features described in this Policy. Access tokens stay on our servers and are not returned to your browser. They are transmitted to Meta over encrypted connections and may be refreshed while your connection remains active.

Removing iDeep in Instagram’s Apps and Websites settings deauthorizes the connection and removes the associated access token from our active database. It does not delete your separate iDeep account or its non-Instagram content. To delete all account data, use the deletion methods below.

Retention

Account, brand, connection and content records are generally retained while your account is active. One-time sign-in codes become unusable after 10 minutes. OAuth state and rate-limit records expire and are periodically removed. Public website reads and extracted metadata are cached for up to approximately 24 hours and may be stored separately from your account during that period.

After deletion, limited security, fraud-prevention, diagnostic, legal or transaction records may remain only where reasonably necessary or legally required, and backup or provider copies may take a limited period to expire. We delete or de-identify such records when no longer needed. Content already published to Instagram remains subject to Instagram’s controls and policies; deleting iDeep does not delete it from Instagram.

Deletion and your choices

You may delete your iDeep account by signing in, opening Settings, and selecting **Delete account**. You may also request access, correction or deletion by emailing privacy@ideep.app from your account email address. See our [Data deletion instructions](#). We may need to verify your identity before completing a request.

Depending on where you live, you may also have rights to receive a copy of your data, restrict or object to processing, withdraw consent, or complain to a data-protection authority. We will not discriminate against you for exercising applicable privacy rights.

Security and international processing

We use reasonable administrative, technical and organizational safeguards designed to protect information, including access controls, server-side token storage and encrypted transport. No internet service can guarantee absolute security. The Service and its providers may process information in countries other than your own; where required, we use legally recognized transfer safeguards.

Children

The Service is intended for businesses and is not directed to children under 18. We do not knowingly collect personal information from children. Contact us if you believe a child has provided personal information through the Service.

Changes and contact

We may update this Policy as the Service or law changes. We will post the updated version here, change the date above and provide additional notice when required. We retain prior versions as required by applicable platform rules. For privacy requests, questions or security reports, contact privacy@ideep.app.