

Privacy Policy

Effective Date: May 20, 2026

This Privacy Policy describes how Brez Marketing LLC ("Company," "we," "us," or "our") collects, uses, stores, shares, and protects your information when you use AdLevel (the "Service") — a business-to-business advertising management platform that helps you create, launch, and optimize advertising campaigns on connected Meta ad accounts.

This policy is written to comply with the General Data Protection Regulation (GDPR), the UK GDPR, the California Consumer Privacy Act as amended by the CPRA (CCPA/CPRA), other U.S. state privacy laws, Meta Platform Terms and Developer Policies, and the Apple App Store and Google Play Data Safety requirements.

AdLevel is not endorsed, certified, or otherwise approved by Meta Platforms, Inc. or Facebook.

1. Information We Collect

1.1 Account Registration & Authentication

AdLevel uses email/password authentication via Supabase Auth as the primary sign-in method, with optional Whop OAuth (for users who purchased AdLevel through a Whop community) as a secondary sign-in method. We do *not* use Facebook Login for authentication.

When you create or sign in to an AdLevel account we collect:

- Email address (required for sign-in and service communications)
- Encrypted password hash (Supabase Auth — we never see your plaintext password)
- Full name, optional phone number, optional avatar, optional workspace/business name and timezone — as provided in your Profile
- Multi-factor authentication factors (TOTP secret and one-time backup codes) if you enable MFA
- If you signed in through Whop: your Whop user ID, Whop membership ID, and the email and name on file with Whop

1.2 Meta Ad-Account Connection (separate from sign-in)

After you create an AdLevel account, you may optionally connect one or more Meta (Facebook) ad accounts via Meta's Marketing API OAuth flow. This is a separate authorization event from sign-in. When you complete the Meta OAuth flow we store:

- A long-lived Meta access token (stored encrypted; see §4)
- Your Meta user ID — required so Meta can identify you when you request data deletion from facebook.com/settings (see §6)

- The ad accounts you selected (account ID, name, currency, timezone, status, spending limits) and the Facebook Pages you manage

We do *not* request the `email` or `public_profile` Facebook Login scopes. As a result Meta does not share your Facebook display name, email, or profile picture with us through the OAuth flow.

1.3 Meta Marketing API Data

Once an ad account is connected, AdLevel reads and (with your authorization) writes the following business data via the Marketing API:

Ad Account Data:

- Ad account ID, name, status, currency, timezone, and spending limits
- Account-level billing and spend summaries

Campaign Data:

- Campaign, ad set, and ad IDs, names, objectives, statuses, budgets, and schedules
- Targeting parameters (audiences, locations, age, interests) and optimization goals you set
- Ad creative content (text, headlines, descriptions, image and video references)

Performance Insights:

- Impressions, reach, frequency, clicks, CTR, CPC, CPM
- Leads, cost per lead, and conversion actions configured by you
- Spend totals (daily and lifetime, per campaign / ad set / ad)

Business & Page Data:

- Facebook Page name and ID
- Business Manager / Business Portfolio ID and name
- Ad pixel IDs and names (for conversion tracking)
- Lead form names, statuses, and lead counts (for lead-generation campaigns)

1.4 Content You Create in AdLevel

- Free-text prompts and questions you send to our AI assistant ("Athena") and follow-up chat history. If you use the iOS or Android keyboard's built-in dictation to enter that text, the speech-to-text conversion is performed by your operating system; AdLevel only receives the resulting text.
- Images you upload (e.g. product photos) for use in ad creatives
- Support tickets, attachments, and correspondence with our team
- Onboarding answers (monthly ad spend range, industry, optimization metric, creative-test frequency)

1.5 Automatically Collected Technical Data

- IP address, user-agent, device information, and operating system
- Pages visited within AdLevel (only after you accept analytics — see §7)
- Server logs (API calls, error logs, timestamps) used for security and debugging
- Mobile-only: Expo push token (a device identifier provided by Apple or Google) so we can send you alerts
- Mobile-only: a flag stored in the device Keychain indicating whether biometric unlock is enabled

1.6 Billing Data

Payments are processed by Whop. We do *not* receive or store full card numbers, expiry dates, or CVCs. Whop returns your Whop user ID, membership ID, and subscription/payment status to AdLevel via webhook so we can determine whether your account is active. We retain transaction history (date, amount, type, balance after transaction) for tax/legal compliance.

2. Meta Permissions Requested

When you connect a Meta ad account, AdLevel requests the following permissions. We only request what is necessary for AdLevel's core functionality.

Permission	Purpose
ads_management	Create, edit, pause, and manage campaigns, ad sets, and ads on your behalf
ads_read	Read campaign structure, performance metrics, and analytics
pages_show_list	List Facebook Pages you manage so you can select one for ad creation
pages_manage_ads	Create and manage ads linked to your Pages and access lead-form data
pages_read_engagement	Read Page metadata, profile picture, and post content for campaign configuration
business_management	Access Business Manager / Business Portfolio information and associated ad accounts

You can review and revoke these permissions at any time from facebook.com → Settings → Business Integrations, or by disconnecting the ad account in AdLevel Settings → Ad Accounts.

3. How We Use Your Data

3.1 Service Operation

- Provide and operate the Service: account management, ad-account integration, dashboards, reporting, and the AI assistant (Athena)

- Authenticate your identity and protect your account (MFA, suspicious sign-in detection, session management)
- Communicate with you about the Service (transactional emails: welcome, security, billing, support replies)
- Generate AI-driven recommendations and, where you enable it, allow our autonomous Campaign Agent to pause/activate/modify ad sets and adjust budgets within thresholds you have approved (see §3.4)
- Send mobile push notifications you have opted in to (account alerts, agent activity)
- Detect, prevent, investigate, and address fraud, abuse, security incidents, and technical problems
- Comply with legal obligations and respond to lawful requests

3.2 AI Processing

Athena (our AI assistant) sends the text of your prompts, follow-up messages, and the contextual information needed to answer (e.g. a campaign's name and recent metrics) to large-language-model providers — currently OpenAI and Anthropic — over their commercial APIs. Images you upload to Athena are sent to OpenAI for vision analysis and may be sent to Runware for image generation/editing.

We currently operate on the default API tier with our LLM providers. Under that tier, OpenAI and Anthropic may retain API payloads for up to 30 days to monitor for abuse, after which they are deleted. Neither provider uses our API content to train their public models. We rely on commercial Data Processing Agreements (DPAs) and Standard Contractual Clauses with each provider.

3.3 What We Do NOT Do

- We do **not** sell or “share” (as defined in the CCPA/CPRA) your personal information
- We do **not** use your ad-account data to run our own advertisements
- We do **not** share your campaign data with other AdLevel users
- We do **not** use your data to build user profiles for cross-context behavioral advertising
- We do **not** transfer Meta data to data brokers or advertising networks
- We do **not** use your data to train generative-AI base models

3.4 Autonomous Campaign Agent — Important Notice

If you enable the autonomous Campaign Agent, AdLevel will use AI inference to pause, activate, or modify your campaigns, ad sets, and ads — including changes to daily budgets — on your behalf, without per-action confirmation. The Agent operates within boundaries you configure (e.g. budget-change approval threshold). You can disable the Agent at any time in Settings, after which campaign changes will require manual confirmation. AI inferences may be imperfect; you remain solely responsible for your ad spend. See the Autonomous Agent Disclosure in our Terms of Service for additional detail.

4. How We Store & Protect Your Data

4.1 Storage

- All structured data is stored in Supabase (Postgres) hosted in the United States
- Database connections use TLS 1.2+ in transit; database storage is encrypted at rest by the underlying cloud provider
- Meta access tokens are encrypted application-side using AES-256-GCM before they are written to the database. The decryption key is held in our infrastructure secrets manager and rotated periodically.
- Multi-factor authentication secrets (TOTP) and recovery codes are stored as one-way hashes; we cannot read them after enrollment
- Database backups are managed by Supabase per our project tier (default 7-day point-in-time recovery, plus daily backups) and are encrypted at rest

4.2 Security Measures

- TLS 1.2+ for all network connections, including those to third-party APIs
- Row-level security (RLS) on application tables: clients can only read their own rows, and writes happen through our API which authorizes every request
- Production database writes that touch sensitive columns are gated by service-role credentials kept in a secrets manager
- MFA is available for all users and required for administrative access
- Application-level logging redacts known sensitive fields (tokens, secrets, credentials) before any log is written
- Routine vulnerability scanning of our dependency tree and weekly review of advisories from the Node.js, pnpm, and npm security advisories databases

4.3 Data Retention

- Active accounts: We retain your data for as long as your account is active and your ad accounts are connected.
- Account deletion: When you delete your account in Settings, or when Meta sends a deletion-callback request, we begin deletion immediately. We complete deletion of identifiable data from primary systems within 30 days.
- Backups: Identifiable data persists in encrypted backups until the rolling backup retention window expires (typically within 35 days for Supabase point-in-time-recovery, after which the data is overwritten or deleted as part of the standard backup rotation).
- Legal/financial records: Billing transactions and credit-ledger entries are retained in anonymized form (with your user reference set to null) for as long as required by U.S. tax and accounting rules.

- System logs: Application logs are retained for up to 90 days. Logs are written with sensitive fields redacted at source.

5. How We Share Your Data — Sub-processor List

We engage the following sub-processors to operate the Service. Each sub-processor is contractually bound by a Data Processing Agreement (DPA) that restricts use of your data to providing the listed service to us. We rely on Standard Contractual Clauses for transfers from the EEA/UK/Switzerland to providers in the United States.

Sub-processor	Purpose	Region
Supabase	Database, authentication, file storage	United States
Vercel	Web hosting and (with consent) analytics	United States
Railway	Background worker hosting (BullMQ + Redis)	United States
OpenAI	Primary LLM for Athena (chat content, vision); default 30-day API retention	United States
Anthropic	Reasoning model for the autonomous Campaign Agent; default 30-day API retention	United States
Runware	AI image generation and editing for ad creatives	European Union
Whop	Billing, subscriptions, and optional OAuth sign-in	United States
Resend	Transactional email (welcome, billing, support, security)	United States
Expo Push Service	Mobile push notification relay (forwards to Apple APNs and Google FCM)	United States
Apple Push Notification service (APNs)	iOS push delivery	United States
Google Firebase Cloud Messaging (FCM)	Android push delivery	United States / European Union
Meta Platforms (Marketing API)	Connected ad-account operations (outbound only)	United States

5.1 Legal Disclosures

We may disclose your information if required by law, subpoena, court order, or government request, or if we reasonably believe disclosure is necessary to protect our rights, the safety of users, or the public.

5.2 Business Transfers

If we are involved in a merger, acquisition, or sale of all or part of our assets, your data may be transferred as part of that transaction. We will notify you by email and a prominent in-product notice before any transfer that changes the controller of your data.

6. Deleting Your Data

6.1 In-app account deletion

You may delete your account at any time from Settings → Privacy → Delete account (adlevel.ai/settings?tab=privacy). Deletion revokes your connected Meta access tokens with Meta, removes all your campaigns, chat history, support tickets, push tokens, uploaded files, and profile, and deletes your Supabase Auth record. Financial transaction records are anonymized but retained for tax/legal compliance.

6.2 Removing the app from Facebook

You may also remove AdLevel from your Facebook account at facebook.com → Settings → Business Integrations. Doing so revokes AdLevel's API access immediately. To delete the data we already hold about you, follow the instructions on our Data Deletion Instructions page at adlevel.ai/deletion (the URL we list in Meta's App Dashboard as our "User Data Deletion Instructions URL") or use Settings → Privacy → Delete account.

We additionally operate a Data Deletion Callback endpoint at <https://adlevel.ai/api/data-deletion-callback> that accepts Meta-signed deletion requests. If Meta sends one for your Facebook user, the endpoint verifies the signature against our Meta App Secret, queues full deletion of any matching AdLevel account, and returns a confirmation URL of the form <https://adlevel.ai/deletion/status/<code>> where you can check status.

6.3 Other deletion paths

You can also email support@adlevel.ai with "Data Deletion Request — AdLevel" in the subject. See our Data Deletion Instructions page (adlevel.ai/deletion) for the full set of options.

7. Cookies & Analytics

- **Essential cookies** (always on): Supabase session cookies (`sb-*`), OAuth PKCE/state cookies during sign-in, MFA flow state cookies. These are needed for the Service to work and cannot be disabled.
- **Vercel Analytics** (opt-in): If you accept the cookie banner, we load Vercel's privacy-focused pageview analytics, which records the page URL, anonymized IP, user-agent, and session timing. Analytics is *off* until you accept and can be reset from Settings → Privacy.

We do not load the Meta Pixel, Facebook SDK, or any cross-site tracking pixel on AdLevel. We do not use cookies to track your activity outside of AdLevel.

8. International Data Transfers

Brez Marketing LLC is based in Miami, Florida, USA. Our primary database (Supabase) is hosted in the United States. If you access AdLevel from outside the United States, your data is transferred to and processed in the United States, and may also be processed in the European Union by sub-processors listed in §5.

For users in the European Economic Area (EEA), United Kingdom, or Switzerland: we rely on the European Commission's Standard Contractual Clauses (SCCs) and, where applicable, the UK International Data Transfer Addendum, as the lawful transfer mechanism. Each sub-processor in §5 has signed a DPA that incorporates SCCs.

9. Your Rights

9.1 EEA / UK / Switzerland (GDPR & UK GDPR)

If you are located in the EEA, the UK, or Switzerland, you have the following rights:

- Right of access — request a copy of the personal data we hold about you (in-app via Settings → Privacy → Download my data)
- Right to rectification — update inaccurate data (in-app via Settings → Profile)
- Right to erasure — delete your account and associated data (in-app via Settings → Privacy → Delete account)
- Right to restrict processing — request that we limit how we use your data
- Right to data portability — receive your data in a structured, machine-readable format (the in-app export delivers JSON within a ZIP archive)
- Right to object — object to processing based on our legitimate interests
- Right to withdraw consent — withdraw consent at any time where processing is based on consent (e.g. analytics cookies, optional Whop OAuth, Meta ad-account connection)
- Right to lodge a complaint — with your local Data Protection Authority

Legal bases under GDPR Art. 6: (a) contractual necessity for providing the Service to you; (b) your consent for optional integrations (Meta ad-account connection, analytics cookies, marketing email if and when offered); (c) our legitimate interests in service improvement, security, abuse prevention, and product analytics; and (d) compliance with legal obligations.

9.2 California (CCPA / CPRA)

- Right to know — request the categories and specific pieces of personal information we collect, the purposes for collection, and the categories of recipients

- Right to delete — request deletion of your personal information (in-app via Settings → Privacy → Delete account)
- Right to correct — request correction of inaccurate personal information
- Right to opt out of sale or sharing — we do **not** sell or share (as those terms are defined in the CCPA/CPRA) your personal information; no “Do Not Sell or Share” link is required
- Right to limit use of sensitive personal information — we do not use sensitive personal information except as necessary to provide the Service
- Right to non-discrimination — we will not discriminate against you for exercising your rights

9.3 Other U.S. State Residents

Residents of states with comprehensive privacy laws — including but not limited to Virginia (CDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), Texas (TDPSA), Oregon (OCPA), Iowa, Indiana, Tennessee, Montana, Florida, New Jersey, Delaware, and New Hampshire — have rights similar to those listed under CCPA above, including the right to access, delete, correct, port, and (where applicable) opt out of profiling or targeted advertising. We honor those rights regardless of state, and you can exercise them through the same in-app paths as CCPA users.

9.4 How to exercise your rights

Most rights can be exercised directly from Settings → Privacy (Download my data, Delete account, Reset cookie preference). For anything else, email support@adlevel.ai and we will respond within the timeframes required by applicable law (typically 30 days under GDPR, 45 days under CCPA/CPRA, extendable in limited circumstances).

10. Children's Privacy

AdLevel is intended exclusively for business use by individuals 18 years of age or older who are authorized to manage advertising for a business. We do not knowingly collect personal information from anyone under 18. If you believe a minor has accessed the Service, please contact support@adlevel.ai.

11. Data Breach Notification

In the event of a personal data breach affecting your data, we will notify the relevant supervisory authority within 72 hours of becoming aware, as required by GDPR Art. 33, and we will notify you without undue delay if the breach is likely to result in a high risk to your rights and freedoms. We will also notify Meta and applicable U.S. state regulators where their laws require it.

12. Meta Platform Terms Compliance

Our collection and use of Meta Marketing API data is governed by Meta Platform Terms and Developer Policies. We commit to:

- Only requesting permissions necessary for AdLevel's functionality
- Only using Meta data for the purposes described in this policy
- Deleting Meta data when you remove the app or request deletion (via the live callback endpoint in §6.2)
- Not selling, licensing, or transferring Meta data to data brokers or advertising networks
- Not using Meta data to build user profiles for purposes unrelated to AdLevel
- Maintaining encryption-in-transit, encryption-at-rest, and access controls (see §4)
- Promptly notifying Meta of any data breach involving Meta data

13. Mobile Application Data

The AdLevel mobile app (iOS and Android) requests the following device permissions when you opt to use the related features. None of these permissions is requested on first launch — each is requested only when you tap the corresponding action.

- **Camera** — to take product photos to share with Athena
- **Photo library** — to attach existing photos to Athena conversations
- **Face ID / biometric unlock** — to unlock the app. Biometric data never leaves the device; only a Keychain flag indicating that biometric unlock is enabled is stored.
- **Push notifications** — to alert you about agent activity and account health. The Expo push token is stored on our servers and forwarded to Apple APNs or Google FCM for delivery.

AdLevel does not request microphone or speech-recognition permissions. If you prefer to dictate rather than type, use the built-in dictation key on your iOS or Android keyboard — that runs entirely in the operating system, and AdLevel only ever sees the resulting text.

You can revoke any of these permissions in iOS Settings → AdLevel or Android Settings → Apps → AdLevel. Revoking a permission disables the corresponding feature but does not delete data already collected; use Settings → Privacy → Delete account for that.

14. Marketing Communications

We currently send only transactional emails (welcome, billing, security, support replies, agent alerts). If we add a marketing or promotional email program in the future, you will be opted out by default and can change your preference at any time. Marketing emails will include a one-click unsubscribe link. Transactional emails are not subject to opt-out because they are required to operate your account.

15. Changes to This Policy

We may update this Privacy Policy from time to time. When we make material changes we will update the Effective Date at the top of this page, notify you by email if we have your address, and post a prominent in-product notice. Your continued use of AdLevel after the changes take effect constitutes acceptance of the updated policy. If you do not agree, please delete your account before the changes take effect.

16. Contact

- Company: Brez Marketing LLC
- Location: Miami, Florida, USA
- Privacy contact: support@adlevel.ai
- Data deletion: adlevel.ai/deletion or in-app at Settings → Privacy
- Website: adlevel.ai