CliqWave - Privacy Policy

Effective Date: March 22, 2026

Last Updated: March 22, 2026

This Privacy Policy explains how Greek Time Corp. ("Greek Time," "CliqWave," "we," "our," or "us") collects, uses, discloses, and protects information about you when you use our CliqWave mobile applications, websites, and related services (collectively, the "Services"). This policy also explains how we use analytics, cookies, software development kits ("SDKs"), pixels, and similar technologies on our website and in our mobile applications.

If you do not agree with this policy, please do not use the Services. If you are located in a jurisdiction that requires consent for certain processing, we will rely on the consent choices, device settings, browser settings, and other controls described in this policy where applicable.

Quick Summary

- We collect the information we need to provide, secure, support, and improve the Services, including account details, organization and profile data, messages and media you choose to share, device and app information, and business-contact or lead information.
- Precise location is opt-in and used only for features you enable.
- We use hosting, infrastructure, support, analytics, security, communications, customer-relationship, and advertising/measurement tools to operate the Services and understand the effectiveness of our website, app, campaigns, and onboarding flows.
- On the website, we may use cookies, pixels, local storage, session-replay, and similar technologies, including technologies provided through Google Tag Manager and vendors such as Google Analytics, Microsoft Clarity, LinkedIn, Meta, TikTok, Amplitude, Cloudflare, and similar providers.
- In the mobile app, we may use analytics, diagnostics, crash-reporting, performance, attribution, and advertising/measurement SDKs or APIs, including tools from providers such as Google/Firebase, Amplitude, Microsoft Clarity, Meta, TikTok, and similar vendors, subject to your device, platform, region, and applicable law.
- Where enabled and permitted by law, advertising and measurement partners may receive identifiers, cookie data, device and browser data, app event data, and related interaction signals. On the website, if advanced matching or similar features

are enabled, those partners may also receive hashed or otherwise transformed matching signals derived from information you submit, such as contact information, where supported by the page or form.

- We do not sell personal information for money. However, when we use third-party advertising or measurement tools, certain disclosures of identifiers and internet or other electronic network activity may be considered "sharing" or use for cross-context behavioral advertising under California law.
- In Europe, the UK, Switzerland, and other jurisdictions with similar rules, optional advertising, analytics, and measurement tags on our website remain off until you grant consent where required by law.
- You can request access, correction, deletion, portability, or certain opt-outs as described below. On the website, we also honor Global Privacy Control signals where supported in our implementation.

1) Who We Are & How to Contact Us

Controller: Greek Time Corp.

Address: 1001 S Harrison, West, TX 76691

Email (privacy): privacy@cliqwave.com

Support: support@cliqwave.com

2) Scope

This policy covers information we collect when you:

- use the CliqWave mobile app or website;
- communicate with us, including support requests, demos, waitlists, surveys, feedback, partnership inquiries, event scans, giveaways, or lead forms;
- participate in events, promotions, beta tests, onboarding activities, or campaigns that we host or support; or
- interact with our emails, landing pages, app-store pages, ads, or related digital properties.

This policy does not cover third-party sites, apps, or services you access through the Services, such as external links, app stores, payment providers, identity providers, calendar providers, map providers, or websites controlled by another company. Those parties' privacy practices are governed by their own notices and terms.

3) Information We Collect

We may collect the following categories of information:

- **Account and profile information:** name, email address, username, password hash, organization affiliation, profile photo, role, settings, and similar account details.
- **Organization and activity information:** memberships, roles, events, attendance or check-in records, points, approvals, acknowledgements, calendar data, invitation links, and related service activity.
- **Content you provide:** messages, announcements, polls, uploads, files, images, videos, support messages, demo or intake information, and other content you choose to send, post, upload, or store through the Services.
- **Device, app, website, and usage data:** IP address, approximate location derived from IP, device identifiers, app instance or browser identifiers, operating system, browser type, language, app version, crash data, performance metrics, page URLs, referrers, timestamps, clicks, scrolls, page or screen views, session data, and interaction or diagnostic events.
- **Advertising, attribution, and measurement data:** cookie identifiers, first-party or third-party cookie data, pixels, tags, campaign parameters, ad click identifiers, landing-page information, conversion events, engagement signals, and related analytics or attribution data.
- **Location information:** if you grant location permission, we may collect precise or near-precise location for features such as check-ins, maps, or location-based experiences.
- **Business and marketing information:** lead-source details, campaign metadata, CRM records, communication history, organization interest, demo status, newsletter preferences, and similar contact or marketing data.
- **Third-party and integration data:** if you use sign-in, calendar, map, payment, app-store, or other integrations, we may receive the limited information needed to support that integration.
- **Sensitive information:** depending on how you use the Services, we may process sensitive information such as precise geolocation (if enabled by you), account credentials, and the content you choose to submit through the Services. We do not use sensitive personal information to infer characteristics about you.

You should not upload unlawful content or sensitive information that is not necessary for your use of the Services.

4) Sources of Information

We collect information:

- directly from you;

- automatically from your devices, browser, app, cookies, SDKs, tags, pixels, logs, and similar technologies;
- from organizations, administrators, and members using the Services;
- from advertising, analytics, attribution, and CRM providers acting on our behalf or with whom we work;
- from app stores, identity providers, calendar providers, hosting providers, and other integrations you choose to use; and
- from publicly available sources or event/lead sources where permitted by law.

5) How We Use Information

We use information to:

- provide, operate, maintain, and improve the Services;
- authenticate users and organizations, manage memberships, and support events, messaging, content sharing, points, calendars, attendance, and related workflows;
- protect users, organizations, and the Services, including fraud prevention, abuse detection, moderation, security investigations, and incident response;
- debug, test, monitor reliability, understand product performance, and improve user experience;
- measure website and app usage, campaign performance, traffic sources, audience engagement, conversion activity, and onboarding effectiveness;
- communicate with you about service updates, support issues, onboarding, lifecycle messaging, newsletters, or promotions, subject to applicable law and your choices;
- manage leads, demos, customer relationships, and business operations, including CRM and campaign administration;
- comply with legal obligations, enforce our terms and policies, and protect our rights or the rights and safety of others; and
- create aggregated, de-identified, or statistical reporting where permitted by law.

6) Analytics, Advertising, Cookies, SDKs, and Similar Technologies

We may use analytics, crash-reporting, performance, attribution, product-experience, session-replay, cookie, local-storage, pixel, SDK, and similar technologies to understand usage, improve performance, secure the Services, support operations, and measure our marketing.

Examples of tools or categories we may use include:

- infrastructure and delivery tools such as AWS, Google Cloud Platform, Firebase, Cloudflare, and similar providers;
- analytics and product-experience tools such as Google Analytics, Amplitude, Microsoft Clarity, and similar providers;
- customer-relationship, communications, or lead-management tools such as Odoo and related email or communications providers; and
- advertising, attribution, and measurement tools such as LinkedIn Insight Tag, Meta Pixel or related business tools, TikTok Pixel or related business tools, and similar providers.

On our website, these technologies may collect information such as IP address, user agent, page URLs, referrers, time stamps, landing-page views, page views, button clicks, scroll depth, session events, cookies, and similar online identifiers. Where advanced matching or similar features are enabled, advertising or measurement partners may also receive hashed or otherwise transformed matching signals derived from information submitted through a page or form, such as email address, phone number, name, address, or external identifiers, where supported and permitted by law.

In our mobile applications, these technologies may collect information such as app instance identifiers, device and operating-system details, app version, crash and performance data, installation and app-open signals, attribution signals, and in-app event data. Depending on your device, platform, app settings, region, and applicable law, some mobile analytics or advertising-related collection may be disabled, limited, or configured differently.

7) Region-Based Controls, Consent, and Browser Signals

We apply different controls depending on the surface you use, the technologies involved, the region we reasonably determine applies to your use, your browser or device settings, and applicable law.

For example:

- on our website, optional analytics and advertising/measurement tags may remain off until you grant consent in regions where consent is required by law;
- if you decline those optional technologies, we keep those technologies off until you later change your choice, subject to the technical limits of the browser or page session;
- where supported in our implementation, we honor the Global Privacy Control ("GPC") browser signal for non-essential website tagging;
- on mobile platforms, certain advertising or measurement features may depend on platform permissions, app settings, region-based defaults, or device-level choices; and

- some strictly necessary or security-related technologies may still operate because they are needed to provide, secure, or maintain the Services.

8) Legal Bases for Processing (EEA, UK, and Switzerland)

If you are in the European Economic Area, the United Kingdom, or Switzerland, we rely on one or more of the following legal bases:

- **Contract:** to provide the Services you request, create and administer accounts, support organizations, process transactions you initiate, and perform our contractual obligations.
- **Legitimate interests:** to secure and improve the Services, prevent abuse, understand product performance, administer our business, respond to inquiries, and measure the effectiveness of our operations and communications in a proportionate way.
- **Consent:** where required, including for optional cookies, pixels, advertising/measurement technologies, certain analytics or replay technologies, certain marketing communications, or other processing for which consent is required by law.
- **Legal obligation:** to comply with applicable laws, regulations, lawful requests, court orders, accounting obligations, and recordkeeping requirements.
- **Vital interests / public interest:** where permitted by law in limited situations involving safety, security, or other urgent circumstances.

Where we rely on consent, you can withdraw it at any time for future processing using the controls available to you.

9) How We Share Information

We may disclose information in the following circumstances:

- **Service providers and infrastructure vendors:** hosting, storage, content delivery, communications, analytics, diagnostics, customer support, security, CRM, and related vendors that process information on our behalf under contractual restrictions.
- **Advertising, attribution, and measurement partners:** to measure website or app activity, attribute traffic or conversions, understand campaign performance, enable or improve audience measurement, and support related advertising or analytics functions. Depending on the laws that apply, these disclosures may be treated as "sharing" or use for cross-context behavioral advertising.
- **Organizations and other users:** your profile, content, activity, and related data may be visible to the organizations, administrators, and members with whom you

interact through the Services, based on the product's functionality and your actions.

- **Legal, safety, and rights-related disclosures:** when reasonably necessary to comply with law, respond to lawful requests, enforce our terms, investigate misuse, or protect the rights, property, or safety of users, organizations, us, or others.
- **Business transfers:** in connection with a merger, acquisition, financing, reorganization, or sale of assets, subject to applicable confidentiality and notice requirements.

We do not sell personal information for money.

10) Data Retention

We retain information for as long as reasonably necessary for the purposes described in this policy, including to provide the Services, maintain records, comply with legal obligations, resolve disputes, and enforce agreements.

Examples:

- account data is typically retained while your account is active and for a reasonable period afterward to support deletion processing, security, backup retention, and legal compliance;
- messages, uploads, and organization records are retained according to product functionality, organizational settings, and operational needs;
- lead, contact, marketing-preference, cookie-consent, and CRM records are retained as needed to manage the relationship, honor choices or opt-outs, document preferences, and support lawful business operations;
- logs, fraud, moderation, and security data may be retained for audit, integrity, abuse-prevention, debugging, and legal purposes; and
- analytics, attribution, and event records may be retained for reporting, fraud prevention, campaign measurement, product improvement, and compliance purposes, subject to the settings and retention practices of the relevant provider and applicable law.

11) Security

We use technical and organizational safeguards designed to protect information, including encryption in transit, access controls, monitoring, and vendor-management practices. No method of storage or transmission is completely secure, and we cannot guarantee absolute security.

12) Your Choices & Rights

Depending on where you live, you may have the right to request access to, correction of, deletion of, restriction of, or a copy of your personal information, to object to certain processing, or to withdraw consent.

You can also:

- manage device permissions such as camera, photos, notifications, microphone, contacts, calendars, and location through your device settings;
- use in-app settings, browser settings, or platform controls where available;
- use website consent or privacy-choice tools where available;
- use Global Privacy Control or similar browser-based preference signals where supported;
- unsubscribe from marketing emails using the unsubscribe link in the message; and
- contact us to request help exercising your rights.

To submit a privacy request, contact privacy@cliqwave.com or visit https://cliqwave.com/data-deletion/.

We may take reasonable steps to verify your identity or authority before processing a request, and we will not discriminate against you for exercising applicable privacy rights.

13) California Privacy Disclosures

For California residents, we collect, use, retain, and disclose the categories of personal information described in Sections 3 through 10.

Categories we may collect

In the preceding 12 months, we may have collected:

- identifiers and contact information;
- customer-record information and account information;
- commercial or transaction-related information, including campaign, lead, or relationship data;
- internet or other electronic network activity information, including browsing, interaction, diagnostic, cookie, and event data;
- geolocation data, including approximate geolocation from IP and precise geolocation if you enable location features;
- audio, visual, or similar information you upload or provide;
- professional or educational information if you provide it in connection with an organization or request; and
- inferences drawn from usage, lead, or account activity.

Categories we may disclose for business purposes

We may disclose the categories above to service providers, contractors, and processors for business purposes such as hosting, security, analytics, communications, CRM, support, and business operations.

Categories we may share with advertising or measurement partners

Depending on the Services you use, your settings, and applicable law, we may share identifiers, online identifiers, cookie identifiers, internet or other electronic network activity information, commercial or relationship information, and related measurement or attribution signals with advertising, attribution, or measurement partners such as Meta, TikTok, LinkedIn, Google, and similar vendors. Under California law, some of these disclosures may be considered "sharing" for cross-context behavioral advertising.

California rights

California residents may have the right to:

- know/access personal information we collect, use, disclose, sell, or share;
- correct inaccurate personal information;
- delete personal information, subject to legal exceptions;
- receive a portable copy of certain personal information;
- opt out of sale or sharing of personal information;
- limit the use and disclosure of sensitive personal information, where applicable; and
- not be discriminated against for exercising privacy rights.

We do not sell personal information for money. We do not use sensitive personal information to infer characteristics about you.

We honor Global Privacy Control where supported in our website implementation. Authorized agents may submit requests on your behalf where permitted by law.

14) EEA / UK / Switzerland Privacy Rights

If you are in the EEA, UK, or Switzerland, you may have the right to:

- access personal data we hold about you;
- request correction of inaccurate personal data;
- request erasure of personal data;
- request restriction of processing;
- object to processing based on our legitimate interests, including certain profiling or direct marketing;
- request portability of certain data;

- withdraw consent at any time where we rely on consent; and
- lodge a complaint with your local supervisory authority or, in the UK, the Information Commissioner's Office.

15) International Data Transfers

We may process and store information in the United States and other countries where we or our service providers operate. Those countries may have data-protection laws that differ from the laws in your country. Where required, we use appropriate safeguards for cross-border transfers, such as contractual protections, standard transfer clauses, or other lawful transfer mechanisms.

16) Children's Privacy

The Services are intended for college-age and adult users and are not directed to children under 13. We do not knowingly collect personal information from children under 13. If you believe a child has provided us personal information, contact privacy@cliqwave.com and we will take appropriate steps.

17) Changes to This Policy

We may update this Privacy Policy from time to time. If we make material changes, we may provide notice through the website, the app, or other appropriate means. Your continued use of the Services after the updated policy becomes effective means the updated policy will apply going forward to the extent permitted by law.

18) Contact

Questions or requests regarding this Privacy Policy may be sent to privacy@cliqwave.com.