

Privacy policy

Last updated: 6 September 2026

How personal data is processed and your privacy rights.

1. Who we are

Wendung is a web and funnel analytics service operated by Alexander Alekseenko, Einzelunternehmer, Virgilstraße 9, 81673 Munich, Germany. This policy explains what personal data we collect, why we process it, and how we handle it under the EU General Data Protection Regulation, or GDPR.

2. Our roles under GDPR

Wendung has two different roles depending on the data involved.

Controller

For our website analytics, dashboard product analytics, account, workspace, billing, security, and communication data, Wendung decides why and how the data is processed.

Processor

For analytics events sent by a customer application through the Wendung SDK, the customer is the controller and Wendung processes the data on the customer's instructions.

3. Account and product data

We collect the following data to create and operate your Wendung account, secure the service, provide support, and manage billing.

Account profile

Name, email address, email verification status, password hash, onboarding state, and account preferences.

Workspace and project data

Workspace names, member and invitation details, project settings, allowed origins, API keys, funnel definitions, usage counters, and plan information.

Authentication and security metadata

Session token records, session expiry, IP address, user agent, verification tokens, password reset requests, and similar security records.

Error and performance diagnostics

When you allow analytics and diagnostics, Sentry receives dashboard error reports and sampled performance traces to help us find and fix problems. Reports can include stack traces, navigation and request details, and browser and device metadata. You can withdraw this choice under Account. API error reporting and performance diagnostics operate separately and can include endpoint details, IP addresses, and account identifiers, including your user ID and email.

Billing data

Stripe customer and subscription identifiers, plan, subscription status, invoice metadata, and payment status. Full card details are handled by Stripe and are not stored by Wendung.

Support and transactional communication

Messages you send us and transactional email metadata needed for account confirmations, password resets, workspace invitations, billing, and service notices.

We process account, workspace, subscription, and related support data to provide the service or take steps you request before a contract, under GDPR Article 6(1)(b). Billing records needed to meet tax and accounting obligations fall under Article 6(1)(c). We rely on Article 6(1)(f) for protecting accounts, preventing abuse, maintaining service availability, and investigating server faults. These interests do not replace consent for optional browser analytics and diagnostics, described below.

The account and billing details requested as required are needed to create your account or provide a paid subscription. Without them, we cannot provide the corresponding service. Optional analytics is not a condition of using the website or dashboard.

4. Analytics event data

When a customer application sends events through the Wendung SDK, Wendung processes that data as a processor for the customer. The customer decides what events, properties, traits, and user IDs to send, and is responsible for having a lawful basis and providing its own privacy notice to end users.

- Event name, event ID, timestamp, batch ID, request ID, project ID, and origin.
- Session ID and the user ID that the customer provides through the SDK, if any.

- Event properties and user traits that the customer includes in the payload.
- SDK version, page URL, and referrer when included in the SDK context.
- Country and city derived from Cloudflare request metadata, plus browser, operating system, and device type parsed from the User-Agent header.
- Ingest request status and delivery diagnostics used to debug event delivery.

Customers can enable automatic pageviews or send them manually. Sites must be registered in the project for web analytics reporting. Full pageviews can include the following data in addition to the event data above.

- Page URL and title. In full collection mode, the SDK sends the current URL, including its query string and fragment. Ingest removes the fragment and retains only allow-listed query parameters and the UTM campaign parameters listed below. The original pathname remains in the event alongside a normalized path used for reports.
- Referrer, referrer domain and channel type, and UTM source, medium, campaign, term, and content parameters.
- Browser, operating system, device type, and screen size, plus country and city derived from Cloudflare request metadata.
- A random visitor identifier and a session identifier generated by the SDK. The visitor identifier is kept in the browser storage of the customer site so repeat visits can be counted as one visitor. It is not derived from the IP address. These identifiers are pseudonymous, not proof that the data is anonymous. If a customer supplies a user ID, the service can associate session activity with that user.
- Session aggregates derived from pageviews, such as entry and exit page, session duration, and bounce state, and hourly totals used for reporting.
- A bot flag derived from the User-Agent header. Requests classified as bots are excluded from reports.

Wendung does not add request IP addresses to analytics event rows. Cloudflare receives the request IP address and User-Agent header when delivering the website and SDK, and when receiving analytics requests. The absence of IP addresses from analytics rows does not mean that infrastructure providers never process or log them. Customers should not send special category data, payment card data, government ID numbers, health data, or other sensitive data through the SDK unless we have explicitly agreed to that in writing.

The SDK also offers an aggregate mode for pageviews while a customer's consent choice is pending. This mode sends the page origin and pathname, the referrer's origin, event timestamps, and event and batch identifiers. Ingest adds country, browser, operating system, device type, and a bot flag. Accepted aggregate events omit visitor and session identifiers,

user traits, custom properties, query strings, fragments, titles, screen dimensions, and city. Individual event records feed the pageview totals. They do not contribute to visitor or session counts.

An aggregate collection mode does not establish a consent exemption. A pathname can still contain personal information. Customers must assess their configuration and applicable law before collecting without consent. Our own website uses the consent-based setup below.

5. Cookies and browser storage

On this website, Wendung analytics stays off until you select Allow. After you allow it, we measure pageviews, returning visitors, sessions, referral sources, and engagement to understand how people use the website. We collect the full pageview data described above, using Cloudflare for delivery and Tinybird for storage and reports. We store a random visitor ID in local storage and a session ID in session storage. We do not attach an account ID to these website pageviews. Your browser downloads the SDK script before you choose, but it sends no analytics events until you allow them.

This optional analytics relies on your consent under GDPR Article 6(1)(a) and § 25(1) TDDDG for browser storage and access. Select Analytics preferences in the footer, then Decline, to withdraw consent. This stops collection, discards unsent events, and removes the SDK's browser identifiers. It cannot recall requests already sent. Withdrawal does not affect the lawfulness of processing based on consent before withdrawal. See Your GDPR rights below for erasure requests concerning previously collected data.

We remember Allow or Decline separately in browser storage so we can respect your choice on later visits. This preference storage serves the consent control under § 25(2)(2) TDDDG. Declining analytics does not prevent the requests needed to deliver pages and protect the service. Cloudflare processes connection data for those requests, including your IP address, requested URL, and HTTP headers.

The Wendung website and dashboard do not use third-party advertising cookies, cross-site tracking cookies, or third-party analytics cookies. The dashboard runs our own SDK to record product steps such as creating a project, and it stays off until you allow it in the notice shown after sign-in or under Account, where you can turn it off again at any time.

The dashboard's optional product analytics and browser diagnostics also rely on consent under GDPR Article 6(1)(a) and § 25(1) TDDDG where browser storage or access is involved. The dashboard's choice is separate from this website's choice. Authentication cookies and the consent preference continue to operate when analytics is off.

wendung.session_token

A strictly necessary authentication cookie used to keep you signed in to the dashboard.

Dashboard local storage

Local browser storage may remember interface preferences such as theme, sidebar state, and selected project. These items are not used for advertising or cross-site tracking.

pageview-consent-v1 and analytics-consent-v2

Your analytics choice for this website and, separately, the dashboard. Each site stores its choice in local storage to remember your preference. These entries contain the choice, not a visitor identifier, and have no automatic expiry. You can change your choice or clear the storage in your browser.

@wendung/sdk/anonymous/v1

After you allow analytics, a random visitor identifier in local storage links visits on the same site. It has no automatic expiry. Declining analytics removes it from that site, and you can also clear it in your browser.

@wendung/sdk/session/v1

After you allow analytics, session storage holds a session identifier and activity timestamps. The SDK replaces the session after 30 minutes without activity or after 24 hours. Closing the tab normally clears session storage. Declining analytics removes this entry.

@wendung/sdk/identity/v1

After you allow dashboard product analytics, local storage holds your user ID so product steps can be associated with your account. This entry has no automatic expiry. Signing out or declining analytics removes it. Our public website does not identify you through an account ID.

6. AI features

Wendung may offer optional AI chat and AI-generated funnel insights. When you use these features, prompts, selected workspace/project context, funnel configuration, aggregated analytics results, and generated responses may be processed by Anthropic so the feature can respond. We do not use AI features for decisions that produce legal or similarly significant effects about individuals.

7. Service providers

We use the following providers to operate Wendung. They process data for the services described below. Their role depends on the service and processing involved. Payment providers may also process data under their own legal obligations.

Cloudflare

Infrastructure, DNS, CDN, Workers, Queues, KV, rate limiting, security, and edge routing.

[Privacy policy](#)

Neon

Application Postgres database for account, workspace, project, billing, and product configuration data. [Privacy policy](#)

Tinybird

Analytics event store, query engine, pageview and session aggregates, ingest request logs, and event delivery diagnostics. [Privacy policy](#)

Stripe

Subscription billing, checkout, invoices, payment processing, and billing portal operations.

[Privacy policy](#)

Resend

Transactional email delivery for account confirmation, password reset, email change, account deletion, workspace invitations, and service messages. [Privacy policy](#)

Inngest

Background job orchestration for scheduled usage syncs and asynchronous insight generation workflows. [Privacy policy](#)

Sentry

Error monitoring and performance tracing for the dashboard and API, including stack traces, request metadata, browser and device metadata, IP address, and the signed-in user ID and email address, processed in the Sentry EU data region. [Privacy policy](#)

Anthropic

AI model provider for optional AI chat and AI-generated funnel insights when those features are enabled or used. [Privacy policy](#)

8. Retention and deletion

Account, workspace, and project data are retained for as long as needed to provide the service, maintain security, resolve disputes, and comply with legal obligations. Billing and tax records may be retained longer where required by law or by Stripe under its own retention rules.

Customer analytics has separate reporting and deletion periods. Reporting windows are 7 days for Free, 30 days for Starter, 90 days for Growth, and 365 days for Scale. Scheduled deletion uses 60 days for Free, 30 days for Starter, 90 days for Growth, and 365 days for

Scale. Some underlying stores expire sooner. Deletion runs in background jobs, so the reporting cutoff is not an instant deletion of every stored copy.

Project owners can request deletion of analytics events, associated delivery logs, and derived pageview and session reports from project settings. Project-level usage totals used for quotas remain separate from this deletion and do not contain visitor or session identifiers.

You can request account deletion from account settings. The self-service action may be blocked while you are the only owner of a workspace with an active or trialing subscription, so that billing and ownership issues can be resolved first. You can still contact us to exercise your statutory erasure rights.

9. Your GDPR rights

Where GDPR applies, you may have the right to request access, rectification, erasure, restriction of processing, portability, objection to processing based on legitimate interests, and withdrawal of consent where processing is based on consent.

You can object to processing based on legitimate interests for reasons relating to your particular situation. Contact us using the address below so we can assess your objection.

Contact us at hello@wendung.app to exercise your rights. We will respond without undue delay and within one month where GDPR applies. For complex or numerous requests, GDPR permits an extension of up to two further months; we will explain the extension within the first month. If your request concerns analytics data that we process for one of our customers, we may need to refer the request to that customer as the controller.

You can lodge a complaint with a supervisory authority, including one in the EU country where you live or work, or where you believe an infringement occurred. Our local authority is [Bayerisches Landesamt für Datenschutzaufsicht \(BayLDA\)](#).

10. International transfers

Wendung is operated from Germany. Some providers may process data outside the EU/EEA. Where this happens, we rely on adequacy decisions, Standard Contractual Clauses, or other transfer mechanisms recognized under GDPR.

Contact us at hello@wendung.app for information about the safeguards applicable to your data and how to obtain a copy.

11. Security

We use technical and organizational safeguards appropriate to the service, including access controls, transport encryption where applicable, password hashing, rate limiting, and infrastructure protections. No internet service can be guaranteed completely secure, but we work to reduce risk and respond to issues promptly.

12. Changes to this policy

We may update this policy from time to time. If we make material changes, we will update the date above and may notify you by email or in-app notice where appropriate.

13. Contact

Alexander Alekseenko
Einzelunternehmer
Virgilstraße 9
81673 Munich
Germany
hello@wendung.app