

Privacy policy

Last updated: 24 October 2026.

This privacy policy explains how WEBAPI GROUP SAS handles personal data for WebAPI Group. WEBAPI GROUP SAS ("we", "us") is a French société par actions simplifiée. SIREN 984 275 917. Headquarters SIRET 984 275 917 00016. VAT number FR32984275917.

Registered with the Trade and Companies Register of Toulouse on 16 February 2024 under number 984 275 917 R.C.S. Toulouse. Share capital EUR 1,000. Registered office: ZI de Vic, 10 ter route d'Escalquens, 31320 Castanet-Tolosan, France. APE code 62.01Z. Its corporate purpose is the design, creation, development, maintenance, and updating of websites, web applications, and digital solutions.

This policy replaces earlier public text that described United States servers for the service, or the EU-US Privacy Shield. We do not rely on the Privacy Shield.

1. Roles

We are the controller for account data, billing, the public website, support, and dashboard security. We are the processor for customer API content, which means API requests, URLs, search queries, video, capture options, chart data, monitoring settings, extracted or generated results, and request logs. You choose the purpose of that customer content. The [data processing agreement](#) sets out the processor terms and applies to every customer.

2. Information we collect

We collect information you give us: name, email address, organisation, account credentials, and support messages. Stripe collects payment-card data. We keep billing references and invoices, not full card numbers.

We collect technical data from the website and the service, such as IP address, browser type, and log data needed to run, secure, and bill the service.

On the dashboard, we collect browser, device, and network signals, including characteristics used to recognise a returning device. The open-source FingerprintJS library runs in your browser. We use these signals to protect accounts and to detect abuse. We do not use them for advertising, and we do not sell them. They are stored on the same infrastructure as the service. A limited security profile built from them may be sent to Mistral AI.

If you use the documentation assistant, or if you open a support ticket, the messages in that conversation may be sent to Mistral AI so we can classify, draft, or answer them. Mistral does not receive the API request stream.

3. Why we use it

We use personal data to provide the service and perform the contract, to take payment, to secure accounts, to answer support requests, to keep legally required records, and, where we ask for consent, to measure the website. Legitimate interests cover security, fraud prevention, and understanding how the website is used, balanced against your rights. We ask for consent before non-essential analytics cookies.

We do not sell personal data.

4. Where processing takes place

Customer API content is processed only in the EU/EEA, on Hetzner infrastructure in Germany (Falkenstein and Nuremberg) and Finland (Helsinki), and in our own datacenters in Toulouse. This applies to every customer and every plan.

Cloudflare, Inc. provides DNS for the public websites. The proxy is enabled on those sites, and Orange-to-Orange is enabled. Cloudflare does not host customer API content. That content stays on Hetzner and in the Toulouse datacenters.

Some account, billing, email, website-analytics, support, and engineering data is handled by the providers on the [subprocessor page](#). Several of those providers are outside the EEA. Those transfers do not include the API request stream. Where a transfer leaves the EEA, we use the European Commission's 2021 Standard Contractual Clauses (Decision 2021/914). The [SCC addendum](#) records the annexes. The competent authority is the [CNIL](#).

5. How long we keep it

We keep account data while the account is open, and afterwards for as long as we need it for security, disputes, or a legal duty. Invoices and accounting records are kept for the period required by French accounting law. Request logs are kept while we need them to provide the service, bill usage, and secure it, and are then deleted or isolated. You can ask us to delete account data. We may keep what the law requires us to keep.

6. Security

We use TLS in transit, access controls, API-key authentication, rate limits, and logging. No method of transmission or storage is perfectly secure.

7. Your rights

If the GDPR or the UK GDPR applies, you can ask for access, correction, deletion, restriction, or a copy of your personal data, and you can object to processing based on legitimate interests. Where we rely on consent, you can withdraw it. You can complain to the [CNIL](#) or to your local authority.

If we process customer API content for our customer, write to that customer first. They are the controller. You can also write to us and we will help our customer respond.

8. Cookies

The website uses cookies that are needed to run it. Optional analytics cookies, including Google Analytics, run only with consent where the cookie banner asks for it. You can refuse non-essential cookies in the banner or in your browser.

9. Changes and contact

We will post changes on this page and update the date above. If a change is material, we will also give notice by email or through the service.

Write to the registered office, or use the contact address published on the product website you use. WEBAPI GROUP SAS, ZI de Vic, 10 ter route d'Escalquens, 31320 Castanet-Tolosan, France.