

GDPR statement

Last updated: 25 October 2026.

This statement describes the personal data WEBAPI GROUP SAS processes as controller for WebAPI Group. Customer API content is a separate role.

In this document

- [1. Who this statement covers](#)
- [2. Controller and processor](#)
- [3. The information we process as controller](#)
- [4. Why we process it and the legal bases](#)
- [5. How long we keep it](#)
- [6. Who we share it with](#)
- [7. Transfers outside the EEA](#)
- [8. Your rights](#)
- [9. Security](#)
- [10. Complaints and contact](#)

1. Who this statement covers

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 statement covers WebAPI Group. The products are Autom, BrowserSolver, CaptureKit, ChartQuery, Flystack, HuntAPI, Piloterr, and Veille. Autom is a SERP scraping API. Each product is an API or software service described on its own website.

It covers personal data we process as controller: accounts, billing, the public websites, support, and dashboard security. It does not describe customer API content. That processing has its own page.

2. Controller and processor

We are the controller for the activities in this statement. We decide why account, billing, website, support, and dashboard security data is processed.

We are the processor for customer API content (API requests, URLs, search queries, video, capture options, chart data, monitoring settings, extracted or generated results, and request logs). You remain the controller of that content. You are responsible for the lawful basis, the notice to your users, and the instructions you give us. What that content is, and where it is processed, is the [EU processing statement](#).

The data processing agreement is the Article 28 contract for that processor role. It applies to every customer and every plan through the terms. Accepting the terms is enough. There is no separate enterprise signature.

3. The information we process as controller

As controller we process:

- Identity and account data you give us: name, email address, organisation, account credentials, and API keys.
- Billing records: invoices and billing references. Stripe collects payment-card data. We do not store full payment-card numbers on our servers.
- Support and contact messages, including a documentation-assistant message and the text of a support ticket.
- Technical data from the public websites and the dashboard, such as IP address, browser type, and the log data needed to run and secure them.
- Dashboard security signals. The open-source FingerprintJS library runs in your browser as first-party code. It is not Fingerprint.com. It is not a subprocessor. We use the 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.
- Website analytics events, where you have accepted non-essential analytics cookies.

Customer API content is not in this list.

4. Why we process it and the legal bases

We rely on the following bases in Article 6 of the GDPR.

Processing	Why	Legal basis
Account, credentials, and API keys	Provide the service you ordered	Contract, Article 6(1)(b)

Processing	Why	Legal basis
Invoices and billing records	Take payment and keep accounting records	Contract and a legal obligation, Article 6(1)(b) and (c)
Support messages and documentation-assistant messages	Answer a request about the service	Contract, including steps before a contract, and legitimate interests in running support, Article 6(1)(b) and (f)
Dashboard security signals	Protect accounts and detect abuse	Legitimate interests, Article 6(1)(f)
Website logs needed to deliver and secure the public sites	Run and protect the sites	Legitimate interests, Article 6(1)(f)
Consented website analytics	Measure the public sites	Consent, Article 6(1)(a)

Legitimate interests are security, fraud prevention, and answering a support request. They are weighed against your rights. We ask for consent before non-essential analytics cookies.

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. You can ask us to delete account data. We may keep what the law requires us to keep.

Invoices and accounting records are kept for the period required by French accounting law.

Support messages are kept while we need them to handle the request, a dispute, or a legal duty, and are then deleted or isolated.

Dashboard security signals are kept while we need them to protect accounts and detect abuse, and are then deleted or isolated.

Consented analytics stops when you withdraw consent. You can refuse non-essential cookies in the banner or in your browser.

API request logs are customer API content. How long they are kept is stated in the EU processing statement.

6. Who we share it with

The providers that process personal data for us are on the [subprocessor list](#).

For the controller activities above, the categories are payments, transactional email, consented website analytics, contact forms, support and internal tools, and delivery of the public websites. Hetzner Online GmbH hosts the cloud portion of the service in the EU/EEA. Our datacenters in Toulouse are operated by WEBAPI GROUP SAS. They are a processing location, not a third-party subprocessor.

The public websites use Cloudflare, Inc. for DNS, delivery, and security. Cloudflare's proxy is enabled on all of these sites, and Orange-to-Orange is enabled.

Mistral AI may process support tickets, documentation-assistant messages, and a limited dashboard security profile. Mistral does not receive the API request stream.

We do not sell personal data.

7. Transfers outside the EEA

Transfers outside the EEA can occur for billing, email, website analytics, support, and internal tools. The safeguard is Commission Implementing Decision (EU) 2021/914. We use Standard Contractual Clauses Modules 2 and 3. Clause 17 is French law. The choices are on the [standard contractual clauses](#) page.

Those clauses are not the mechanism for customer API content, because that content stays in the EU/EEA.

We do not rely on the EU-US Privacy Shield.

8. Your rights

If the 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. Withdrawal does not affect processing that took place before it.

To use a right, write to us. Say which right you are using, and give the email address on the account, so we can find the record. Do not send a password, an API key, or a full payment-card number. We may ask for the information we need to confirm that the data is yours. We answer within the time the GDPR allows.

If the data is in customer API content, we process it 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.

A mandatory consumer right is reserved where it applies.

9. Security

We use TLS in transit. Access is limited to people who need it, and those people are under a duty of confidence. The service uses API-key authentication, rate limits, and logging. Full payment-card numbers are not stored on our servers. When a retention period ends, we delete the data or isolate it.

Dashboard device signals are used to protect accounts. They are not an advertising profile.

No method of transmission or storage is perfectly secure. We do not claim a named certification that we do not hold.

10. Complaints and contact

You can complain to the CNIL. The CNIL is the supervisory authority. You can also bring a claim before a court. French law applies. The courts of Toulouse have jurisdiction, except where a mandatory rule gives you the right to bring a claim somewhere else.

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.