

Data processing agreement

Last updated: 24 October 2026.

This data processing agreement ("DPA") is part of the terms for WebAPI Group. It applies to every customer and every plan. It is the Article 28 GDPR contract between the customer ("you") and WEBAPI GROUP SAS. A countersigned copy is available on request. The service does not depend on a separate enterprise signature.

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.

1. Roles and instructions

You are the controller of customer API content. We are the processor. Customer API content means API requests, URLs, search queries, video, capture options, chart data, monitoring settings, extracted or generated results, and request logs.

We process it only to provide, secure, and bill the service, and as you instruct through the product, the API, and these terms. We will tell you if we believe an instruction breaks EU or Member State data-protection law.

We are an independent controller for account data, billing, the public website, support operations, and dashboard security. Those activities are described in the [privacy policy](#), not in this DPA.

2. Details of processing

The subject matter is the service. Processing lasts for the subscription, and for the deletion period below. The nature and purpose are hosting, transmitting, and returning customer API content, preventing abuse, and measuring usage for billing.

Data subjects are the people identifiable in what you choose to submit, and your users. Categories of data are the contents of customer API content. Special-category data should not be submitted. If you submit it, you confirm you have a lawful basis and that you have instructed us to process it.

3. Our people and security

People who can access customer API content are under a duty of confidence. We apply the measures in the privacy policy: TLS, access control, API keys, rate limits, and logging. We review these measures as the service changes. We do not claim a named certification that we do not hold.

4. Subprocessors

We use the subprocessors listed at [Subprocessors](#). Our own datacenters in Toulouse are our infrastructure, not a third-party subprocessor. Hetzner hosts the cloud portion of the service in Falkenstein, Nuremberg, and Helsinki.

We will give at least 30 days' notice before a new subprocessor starts processing customer API content, by updating that page and by email to the account address. You may object in writing during that period. If we cannot offer a reasonable alternative, you may stop the affected service before the change takes effect.

5. International transfers

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.

We do not transfer customer API content outside the EU/EEA to provide the API. The 2021 Standard Contractual Clauses are not the transfer tool for that processing, because that processing stays in the EU/EEA.

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.

Other providers may process account, billing, email, analytics, support, or engineering data outside the EEA. Those transfers use the provider's data-processing terms and the 2021 Standard Contractual Clauses, Modules 2 and 3 as applicable. The annexes are in the [SCC addendum](#). We do not rely on the EU-US Privacy Shield.

6. Assistance, breaches, and deletion

We will help you, taking into account the nature of the processing, to answer data-subject requests about customer API content, and with a data-protection impact assessment that the service specifically triggers.

We will tell you without undue delay after we become aware of a personal-data breach affecting customer API content, and we will include the information we have that you need for your own notification duties.

When the service ends, we will delete or return customer API content, and delete remaining copies, unless EU or Member State law requires us to keep it. Backups are overwritten on their normal cycle and are isolated until then.

7. Audits

You may audit our compliance with this DPA once a year, on reasonable written notice, during business hours, in a way that does not disrupt the service or expose another customer's data. We may satisfy the audit with written answers and relevant third-party reports we hold. A regulator's audit is not limited by the once-a-year rule.

8. Liability and term

Liability under this DPA follows the liability section of the terms. This DPA lasts for as long as we process customer API content for you. If this DPA conflicts with the terms on a data-protection point, this DPA prevails.

9. How this agreement applies

This DPA is binding when you accept the terms. It applies to every customer and every plan. You do not sign it on this page. A countersigned copy is available on request.

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.