

Data Processing Addendum

CitePatch S.L. · B28263838 · Ramón y Cajal 107, 08024 Barcelona, Spain · legal@citepatch.com
Published at <https://citepatch.com/en/legal/dpa/>

This is the CitePatch Data Processing Addendum. It forms part of the Terms of Service and applies to every account automatically, with no separate signature, whenever CitePatch S.L. processes personal data on your behalf as a processor under the GDPR. This version took effect on 17 October 2026. It replaces the version of 8 September 2026 and corrects what that version said about hosting, security measures and subprocessors, so that it matches the infrastructure actually in use. It has not yet been reviewed by outside counsel, but it binds us as written — and where it commits us to something, that something is already running, not planned.

1. Roles, and what this addendum covers

This addendum applies whenever CitePatch S.L. processes personal data on your behalf. For that data you are the controller and CitePatch is the processor.

- 1.1 Customer content — your pages, your brand facts, the prompts you monitor, the patches we draft, and whatever a connected integration returns to us — is processed on your instructions. That is what this addendum governs.
- 1.2 Account and billing data — who your members are, which plan you are on, your invoices — is processed by CitePatch as a controller in its own right. The Privacy Notice governs that, not this addendum.
- 1.3 Where the Terms of Service and this addendum conflict about the handling of personal data, this addendum governs.
- 1.4 No separate signature is needed: this addendum is part of your agreement from the moment you use the product. If your procurement process needs a countersigned copy, write to legal@citepatch.com and we will sign one.

2. Subject matter, nature, purpose and duration

The processing exists to deliver the service described in the Terms of Service, and for nothing else.

- 2.1 Subject matter: measuring how AI assistants answer prompts about your brand, comparing those answers against your own site and your approved brand facts, drafting patches, and publishing the ones you approve.
- 2.2 Nature of the processing: collection by crawling and by API, storage, structured analysis, transmission to the model and search providers listed in the Subprocessors section below, and transmission to an integration you connected when you approve a patch.
- 2.3 Purpose: providing the service to you. CitePatch does not process customer content for its own purposes, and neither we nor our providers train models on it.
- 2.4 Duration: for as long as your account is active, plus the retention periods stated in the Privacy Notice — or until you delete the organization, whichever comes first.

3. Categories of data subjects and of personal data

Most of what CitePatch handles is not personal data at all. What is, arrives in these shapes:

- 3.1 Data subjects: the members of your organization; people named or quoted on the pages we crawl for you; people named in the AI answers we record; and, if you connect Google Analytics 4 or Search Console, the aggregate audience of the property you connect.
- 3.2 Personal data: names, business email addresses, roles and permissions inside your organization; the identity a connected integration exposes to us; personal data incidentally present in your own site content or in a recorded AI answer; and support correspondence.
- 3.3 Special categories of data are not required by the service and are not wanted. The Acceptable Use Policy instructs you not to submit health, biometric, religious, political, trade-union or sexual-orientation data, and CitePatch does not knowingly process it.
- 3.4 Criminal offence data is not processed.

4. Your instructions, and their limits

CitePatch processes customer personal data only on your documented instructions.

- 4.1 Your instructions are this addendum, the Terms of Service, and what you configure in the product: the domains you connect, the prompts you monitor, the patches you approve.
- 4.2 We will tell you if, in our view, an instruction infringes the GDPR or another EU or member-state data protection law, and we may pause that specific processing until it is resolved.
- 4.3 If EU or member-state law requires us to process beyond your instructions, we will tell you before we do, unless that law forbids the telling.

5. Confidentiality, and who can reach your data

Access is limited to the people who need it to run the service, and it is bound.

- 5.1 Everyone with access to customer personal data is under a written confidentiality obligation that outlives their engagement with us.
- 5.2 Production access is restricted to named staff, each with their own keys and accounts; credentials are never shared.
- 5.3 Inside the product, access to your data is scoped to your organization and enforced on every request, not merely hidden in the interface.
- 5.4 Account-level actions — billing, membership, export, deletion — are restricted to owners.

6. Security measures

These are the measures deployed today — the same ones described in plain language on the Security page. They are our Article 32 commitment, and they will grow with the product rather than being promised ahead of it.

- 6.1 Customer data is stored in the EU: the application servers and the database run on DigitalOcean in Amsterdam (Netherlands), and the object storage that holds exports and evidence runs on Google Cloud in europe-west1 (Belgium).
- 6.2 Encryption in transit (TLS) between your browser and CitePatch and between the application and its database. Object storage, secrets and logs are encrypted at rest by Google Cloud, and the integration credentials you connect are encrypted by the application (AES-GCM) before they are stored.
- 6.3 Platform secrets and API keys live in Google Secret Manager, never in the codebase or in a committed environment file; exported bundles never contain integration credentials.
- 6.4 Sign-in is by emailed link or Google OAuth, so there is no password to reuse or leak; session cookies

are HttpOnly and Secure, and mutating requests reject cross-origin calls.

- 6.5 Application and infrastructure logs, retained for security and incident investigation.
- 6.6 Self-service export and deletion, so recovering or removing your data never depends on our goodwill or our availability.
- 6.7 CitePatch holds no ISO 27001 or SOC 2 certification. We would rather name the controls we actually run than point at an audit we have not had.

7. Subprocessors

You give CitePatch general authorisation to engage the following subprocessors. The list is maintained by hand and kept current.

- 7.1 Infrastructure — DigitalOcean (DigitalOcean, LLC), Amsterdam region: the servers that run the application, the database, the cache and our own answer-capture service. Google Cloud Platform (Google Ireland Ltd.): object storage for exports and evidence and background jobs, in europe-west1 (Belgium); message queue, secret storage, logs and telemetry. Cloudflare: DNS for citepatch.com and delivery of the public marketing site; it does not carry traffic to the application. Google Analytics and Google Tag Manager (Google Ireland Ltd.): audience measurement on the public marketing site and inside the product; until you accept cookies, Analytics runs in Google's consent-denied mode and stores nothing in your browser. Contentsquare (formerly Hotjar): session replay and product-usage analytics inside the app, only after consent. Form fields are masked; invite tokens are never sent as page paths.
- 7.2 Payments and email — Stripe: subscriptions, checkout, invoices and the customer billing portal. Resend: transactional email, including sign-in links, invitations and account notifications. MailerLite: the product newsletter, only for people who opt in to it.
- 7.3 Model and search providers — OpenAI, Anthropic, Perplexity and Google (Gemini, via Google Ireland Ltd.) for answer measurement, together with DataForSEO and SearchAPI.io, which capture the answers AI assistants and search engines give in each market; TypeSafe for answer-type classification of measured responses; OpenAI, Anthropic, Google, DeepInfra, Groq and DigitalOcean (serverless inference) for analysis, content drafting, extraction and the Vera assistant; SerpAPI, DataForSEO, Brave Search and Open PageRank for search-engine, keyword and domain-authority data used as evidence. These receive the prompts and responses being measured and the content being drafted, not your account data, and CitePatch does not permit training on customer content.
- 7.4 Before adding or replacing a subprocessor that processes customer personal data, we will notify account owners by email at least 30 days in advance.
- 7.5 You may object within those 30 days on reasonable data-protection grounds. We will try to resolve it; if we cannot, you may terminate the affected part of the service, or the service, without penalty, with a pro-rata refund of anything prepaid for the remaining term.
- 7.6 Each subprocessor is bound by data protection obligations no less protective than those in this addendum, and CitePatch remains fully liable to you for their performance.
- 7.7 Integrations you connect — GitHub, GitLab, Bitbucket, WordPress, Webflow, Shopify, Contentful, Wix, Google Drive, Google Search Console, Google Analytics 4, Cloudflare, Linear — are not subprocessors: they act on your instruction, with credentials you supply and can revoke.

8. International transfers

The database and your files stay in the EU. Some of the model and search providers we send prompts and drafted content to are based in the United States, and our infrastructure providers, DigitalOcean and Google, have parent companies there.

- 8.1 For those transfers we rely on the safeguards each provider offers — the EU-U.S. Data Privacy Framework or standard contractual clauses, as applicable — together with that provider's own data

processing terms.

- 8.2 We have not completed a documented transfer assessment for every provider, and we will not claim one before we have. Write to privacy@citepatch.com for the current status of a specific provider, and tell us if one is unacceptable to you: we will answer honestly whether the product can run without it.
- 8.3 If a transfer mechanism we rely on is invalidated, we will tell you, and either put an alternative in place or stop sending customer personal data to that provider.
- 8.4 To measure what AI assistants answer in a given market, some measurement queries leave through a network exit point in that market — for example Brazil, Mexico or the United States. That traffic is encrypted end to end, it carries only the prompt being measured and the assistant's answer, and nothing is stored at the exit point.

9. Helping you answer data subjects

Requests normally reach you rather than us, because you are the controller.

- 9.1 Owners have self-service export of everything we hold for the organization, and self-service deletion — usually the fastest way to satisfy an access or erasure request.
- 9.2 Beyond that we will assist you with appropriate technical and organisational measures, taking into account the nature of the processing and what is available to us.
- 9.3 If a data subject contacts CitePatch directly about data we hold for you, we will not answer substantively: we will forward the request to the account owner and tell the person that we have done so.
- 9.4 We will also assist you, on the same basis, with data protection impact assessments and any prior consultation with a supervisory authority.

10. Personal data breaches

If we suffer a breach affecting customer personal data, you will hear it from us, promptly and in plain terms.

- 10.1 We will notify affected account owners without undue delay, and in any case within 72 hours of becoming aware of it.
- 10.2 The notice will say what happened, which categories of data and roughly how many records are affected, what we have done, and what we suggest you do — and it will state plainly what we do not yet know instead of waiting until we do.
- 10.3 We will assist you with your own notification duties to supervisory authorities and to data subjects, and we will not ask you to wait on our investigation before meeting a deadline of yours.
- 10.4 Security events that do not touch personal data, such as a failed intrusion attempt or an outage, are outside the scope of this clause.

11. Audit, and what we can actually show you

We are a small company with no certification to hand you, so this section says what a real audit of us looks like instead of implying one we cannot support.

- 11.1 We make available the information needed to demonstrate compliance with Article 28: this addendum, the Security page, the current subprocessor list, and answers to your security questionnaire from a named person rather than a form.
- 11.2 If that is not enough, you may audit us once in any twelve-month period, on 30 days' written notice, during business hours, under confidentiality and at your own cost — yourself or through an independent auditor who is not a competitor of ours.
- 11.3 An audit may not disrupt the service for other customers and does not extend to another customer's data, or to our providers' own infrastructure — for those we pass on the documentation they give us.

12. Return and deletion, and changes to this addendum

Getting your data out, or having it gone, is a button inside the product rather than a support ticket.

- 12.1 An owner can request a full export at any time, as one archive, downloaded through a link that expires.
- 12.2 An owner can delete the organization outright. Deletion runs as a job that removes every project, measurement, patch and stored credential we hold for it, and the product shows you when it has completed.
- 12.3 Deleting the organization is your deletion instruction; there is no waiting period we impose on top of it. We keep only what an accounting or legal obligation requires — invoices, principally — and we keep no backup copy of it.
- 12.4 We may update this addendum. If a change would reduce your protections we will notify account owners before it takes effect, and the date this version took effect is stated at the top of this page.

Countersignature

Not required: this addendum binds both parties without a signature. Complete it only if your procurement process needs a countersigned copy.

Customer

Name

Title

Date

Signature

CitePatch S.L.

Name

Title

Date

Signature