LEGAL

Data Processing Agreement

Effective November 22, 2026

The short version: when your business sends personal data through VANTRA, we process it only to answer you, never store API content, never train on it, and tell you before any new company handles it.

01 What this agreement covers

This Data Processing Agreement ("DPA") applies when a business or other organization ("Customer") uses the VANTRA API or VANTRA Studio (the "Services") to process personal data on its own behalf, for example personal data of its users or employees that it includes in API requests. It forms part of our Terms & Conditions and applies automatically: no signature is needed. If you need a countersigned copy for your records, email us.

Where this DPA and the Terms disagree on the protection of personal data, this DPA wins. Where the Standard Contractual Clauses apply and disagree with this DPA, the Clauses win.

---

02 Roles

Customer is the controller (or a processor acting for its own controller) of the personal data it sends to the Services ("Customer Personal Data"). VANTRA is its processor, and its "service provider" under the California Consumer Privacy Act. Customer is responsible for having a lawful basis for the data it sends us and for giving any notices its own users need.

For account, billing and website data about Customer's own staff (such as the name and email of the person who signs up), VANTRA acts as an independent controller under our Privacy Policy, not under this DPA.

03 Details of the processing

- Subject matter and purpose: providing the Services, which means running the VANTRA models on Customer's requests, storing Customer's encrypted Studio data, billing, and keeping the Services secure.
- Nature: API prompts, files and answers are processed in memory to answer a request and are not stored. Studio conversations, projects and files are encrypted on Customer's devices before they are saved, so VANTRA stores only ciphertext it cannot read; a message is decrypted on the device and read in memory by the model host only to answer it.
- Categories of data: whatever personal data Customer chooses to include in requests and in Studio, plus request metadata (time, model, result, token counts, cost, duration and a request ID), which never includes content.
- Data subjects: the people whose data Customer includes, such as its users, customers and employees.
- Special categories: the Services are not designed for special-category or highly sensitive data. Customer should only send such data if it has assessed that the measures in this DPA are enough.
- Duration and retention: API content is never stored. Request metadata is kept for 7 days and daily usage totals for billing for as long as the account is active. Studio data is kept until Customer deletes it.

04 How VANTRA handles Customer Personal Data

VANTRA will:

- process Customer Personal Data only to provide the Services and on Customer's documented instructions, which are these Terms, this DPA and Customer's use of the Services, unless the law requires otherwise (in which case we will tell Customer first, unless the law forbids it);
- never use Customer Personal Data, or any Inputs or Outputs, to train or improve any model, whether VANTRA's or anyone else's;
- never sell or share Customer Personal Data (as those words are defined in the CCPA), never use it for any commercial purpose other than providing the Services, and never combine it with personal data we get from other sources, except as the CCPA allows a service provider to;

- make sure everyone at VANTRA who can access Customer Personal Data is bound by confidentiality;
- tell Customer if we believe an instruction breaks data protection law, or if we can no longer meet our obligations under this DPA.

05 Security measures

VANTRA keeps appropriate technical and organizational measures in place, described in more detail on our Security page (vantra.cloud/security). They include:

- HTTPS for every connection, with HSTS, and a strict Content-Security-Policy on the website;
- API content handled in memory only, never written to logs, databases or backups;
- Studio history encrypted on the user's device with AES-256-GCM and a key derived from a passphrase that never leaves the device;
- API keys stored only as SHA-256 hashes, with per-key spending limits, model limits, expiry and instant revocation;
- a database encrypted at rest (AES-256), reached only over TLS, with every query scoped to the signed-in account;
- sign-in through Whop with OAuth and PKCE, secure session cookies, and administrator access limited to VANTRA's owner;
- model hosts bound to keep requests in memory only and never train on them.

06 Subprocessors

Customer authorizes VANTRA to use the subprocessors listed at vantra.cloud/subprocessors. Each one is bound by written terms that protect Customer Personal Data at least as well as this DPA, and VANTRA remains responsible for their work.

We add a subprocessor to that list, and announce it in the feed at vantra.cloud/subprocessors.xml, before it starts handling Customer Personal Data. If Customer objects to a new subprocessor on reasonable data protection grounds, it should email us; we will try to find a solution, and if we cannot, Customer may stop using the affected Service and close its account.

07 Helping Customer meet its obligations

Because API content is never stored, there is nothing for VANTRA to retrieve, correct or delete for an API request. Studio users can download or delete all of their data themselves under "Your data". For anything else, such as a request from a data subject, a data protection impact assessment or a question from a regulator, VANTRA will give Customer reasonable help, taking into account what we can see and hold. If we receive a request from one of Customer's data subjects directly, we will pass it to Customer and not answer it ourselves unless Customer asks us to.

08 Personal data breaches

If VANTRA becomes aware of a personal data breach affecting Customer Personal Data, we will tell Customer without undue delay, by email to its account contact. We will share what we know (what happened, the data and people likely affected, the likely consequences and what we are doing about it) and send more as we learn it, so Customer can meet its own notification duties.

09 International transfers

VANTRA and its subprocessors process data in the United States. Where Customer Personal Data from the European Economic Area, the United Kingdom or Switzerland is transferred to a country without an adequacy decision, the parties agree to the European Commission's Standard Contractual Clauses (Module Two, controller to processor, or Module Three, processor to processor, as fits), with the UK International Data Transfer Addendum and the Swiss adjustments where they apply. They are incorporated into this DPA by reference, with Customer as data exporter, VANTRA as data importer, the optional docking clause and Clause 9 option 2 (general authorization) selected, and the details in "Details of the processing" and "Security measures" above as their annexes.

10 Information and audits

VANTRA will make available the information Customer reasonably needs to show compliance with this DPA, starting with this page, the Security page and the subprocessor list. An independent security audit is planned for the second half of 2027; once it exists, we will share its summary on request. If that information is not enough, or a regulator requires it, Customer may audit VANTRA's compliance at its own cost, with at least 30 days' written notice, no more than once a year, during business hours, and under confidentiality.

11 Deletion at the end

When Customer deletes its data or its account, or uses "Delete everything" in Studio, the data is removed straight away and from backups within 30 days, unless the law requires us to keep certain records, such as invoices. API content needs no deletion because it is never stored.

12 Liability

Each party's liability under this DPA is subject to the limitations in the Terms, except where the law or the Standard Contractual Clauses do not allow that.

13 Changes to this DPA

We may update this DPA to reflect changes in the law or in the Services. We will not reduce the protection it gives Customer Personal Data during a paid term without Customer's agreement. The effective date above shows the latest version, and changes are listed in our changelog.

14 Contact

Questions, objections or a request for a signed copy: email support@vantra.cloud.