VENDORBENCHMARK | SECURITY AND DATA REVIEW GUIDE | PUBLIC

Security and data review guide

Vera AI by VendorBenchmark | For security, privacy and procurement reviewers | July 2026

FOUR THINGS TO KNOW FIRST

- **Tenant isolation is enforced by the database, not the application.** More than 270 customer tables sit under Postgres row-level security, and 39 cross-tenant isolation suites re-prove it in CI on every change.
- **Your contracts are never used to train an AI model, ours or anyone else's.** Anthropic and OpenAI do not train on API data, and the zero-data-retention addendum with Anthropic is signed.
- **Every view and download is on the record,** yours and ours, in an audit trail you can export, stream to your SIEM in signed 15-minute batches, and verify in your own tenant.
- **What is not built is listed as plainly as what is:** SOC 2 Type I is targeted for Q4 2026, and EU residency, customer-managed keys, passkeys and ISO 27001 are not built today.

1. PURPOSE AND HOW TO USE THIS DOCUMENT

This guide collects, in one file, the answers VendorBenchmark gives enterprise security, privacy, legal and procurement teams reviewing Vera AI before purchase. It is written for the reviewer working through a questionnaire: every answer describes something implemented on the platform today, every figure can be checked, and the section on what is not built is as complete as the sections on what is. Nothing in it is aspirational.

The same material is published on the web, where it is kept current, and the web pages govern where this file and a page disagree. The reading order:

1. **Security overview.** https://www.vendorbenchmark.com/security
2. **Security and data FAQ.** https://www.vendorbenchmark.com/security-faq
3. **Data processing addendum.** https://www.vendorbenchmark.com/dpa
4. **Subprocessors.** https://www.vendorbenchmark.com/subprocessors
5. **Terms of service.** https://www.vendorbenchmark.com/terms
6. **Trust center.** https://www.vendorbenchmark.com/trust-center
7. **Responsible disclosure.** https://www.vendorbenchmark.com/security-disclosure

The forwardable version of that list is the security review package at https://www.vendorbenchmark.com/security-review-package.

Documents that sit behind an NDA, the pre-completed security questionnaire, the penetration test executive summary, the policy set and the SOC 2 report when it is issued, are delivered through the trust center's document room: a scoped, expiring, revocable link behind a click-through NDA, with every open written to the audit log. Request it at https://www.vendorbenchmark.com/trust-center or by email to info@vendorbenchmark.com.

2. THE PLATFORM IN ONE PAGE

Vera AI is a multitenant platform on which a customer organization stores its software contracts and receives benchmarks, briefs and negotiation deliverables. The application runs on Vercel, the records live in Postgres and the files in private storage buckets on Supabase, both SOC 2 Type II audited, and all data is hosted in the United States. The enforced numbers below are the figures a reviewer can verify.

FIGURE	WHAT IT IS
270+	customer tables covered by Postgres row-level security
39	automated cross-tenant isolation suites run in CI on every change
60 s	signed download URL lifetime, minted per request, never pre-signed into a page
200 MB	upload cap, with the file's actual byte signature checked, not its extension
12+	character password minimum, screened against known breach corpora before acceptance
1 year	maximum age of API keys and SCIM tokens, stored as SHA-256 hashes
15 min	audit event batches streamed to your SIEM, signed and cursor-tracked
72 h	to hear from us directly once an incident affecting your data is confirmed

The life of a contract on the platform. Validated on arrival: Type allowlist, 200 MB cap, byte-signature check. **Isolated in your tenant:** Row-level security and private storage, enforced by the database. **Every touch logged:** Views and downloads, yours and ours, in an audit trail you can read. **Deleted for real:** Your retention policy, your export, and a hard delete that removes rows and files, with a certificate.

3. ARCHITECTURE AND TENANT ISOLATION

3.1 How is tenant isolation actually enforced?

At the database, not in application code. More than 270 customer tables carry your organization ID on every row, and Postgres row-level security policies enforce the boundary on every query. A session from your organization physically cannot return another organization's rows, even if there were a bug in the application layer. Storage policies on the file buckets mirror the same organization rule. This is the control everything else stands on.

3.2 What happens if there is a bug in your application code?

The database still refuses the rows. Row-level security runs inside Postgres, below the application, so a cross-tenant read attempt returns a row-level denial from the database, not an application error a bug could route around. You can reproduce this yourself in a trial: create two organizations, upload to one, and watch the other organization's session get denied at the API.

3.3 How do you prove isolation keeps working as you ship?

39 automated cross-tenant isolation test suites run in CI on every change. The failing cross-org read is a permanent regression test, not a one-time demo, and we demonstrate it live in security reviews on request.

3.4 Do customers share a database?

Yes, and we say so plainly: this is a multitenant Postgres database, not a database per tenant. The boundary is enforced by the database engine through row-level security on more than 270 customer tables, and re-proven by 39 CI isolation suites on every change. What you get is a boundary that is tested continuously rather than assumed per instance.

3.5 Are files isolated the same way as database rows?

Yes. Contract files live in private storage buckets whose policies mirror the organization rule from the database. There is no public URL to any customer file, ever, and access outside your organization is refused even with a direct storage path.

4. IDENTITY AND ACCESS

4.1 What multi-factor authentication do you support?

App-based TOTP, with session step-up enforcement for sensitive actions. Organization owners can enforce MFA org-wide by policy, and MFA is mandatory for every member of VendorBenchmark staff. Passkeys and WebAuthn are not built yet; TOTP is the second factor today.

4.2 Do you support single sign-on?

SAML and OIDC SSO per organization. The Require SSO switch is a real enforcement: once it is on, password and magic-link sign-in are refused for your domain. Organization owners keep a break-glass path so a broken identity provider cannot lock the tenant out.

4.3 Do you support SCIM provisioning?

SCIM 2.0, working today with Okta, Microsoft Entra and any SCIM-capable identity provider: provision, list and deactivate from your directory. Offboarding in your directory is offboarding here. SCIM tokens are stored as SHA-256 hashes and expire within one year.

4.4 What are the password rules?

Twelve characters minimum, and every new password is screened against known breach corpora before acceptance, using a privacy-preserving k-anonymity range query in the style of Have I Been Pwned, so the password itself never leaves our server. Under Require SSO, password sign-in is refused entirely for your domain.

4.5 What are the session lifetimes and session controls?

Users see every active session under Settings, can revoke any single one, or sign out everywhere else with one action. A sign-in from a new device emails the account owner. Organization owners can also set a session policy under Settings: a maximum session age and an idle timeout, so your own limits apply to every member.

4.6 Can we restrict access to our corporate network?

Yes. Organization owners can set an IP allowlist in CIDR notation under Settings, so sessions outside your listed ranges are refused for your organization.

4.7 How do roles and per-contract access work?

Owner and member roles per organization, managed by your own organization owners. Sensitive actions, member management, data export, retention and deletion among them, are owner-only. Below the role layer, individual contracts can be restricted to named people within your organization, so need-to-know applies inside the tenant boundary too.

4.8 Can a customer account become a platform admin?

No. Platform admin rights live in a separate table that no customer-facing code path can write to. There is no privilege-escalation route from a customer account, and admin status cannot be self-assigned.

4.9 How are API keys and SCIM tokens protected?

Both are stored as SHA-256 hashes: we can verify them, nobody can read them back, including us. Both expire within one year, so a forgotten credential ages out on its own. API key management is owner-only.

5. DATA LIFECYCLE, UPLOAD TO DELETION

5.1 What is validated when a file is uploaded?

Three checks before anything else touches it: document types only (PDF, Word, Excel, CSV), a 200 MB cap, and a check of the file's actual byte signature rather than its extension, so a renamed executable is rejected even if it claims to be a PDF. The upload is then written to a private bucket under your organization's path and recorded in the audit trail.

5.2 What information do you collect about individuals?

For your authorized users: name, work email, the timezone they set, and the sign-in credential (a password hash, or nothing when you use SSO). Beyond that, the platform records only what operating it securely requires, and nothing for marketing or profiling.

Audit and session records: the IP address, user agent and time of each sign-in and each action on contract data, and the devices a user is signed in on, kept so your owners can inspect the trail
Activity attribution: which user ran which benchmark, AI analysis or export, in your own tenant
Voice and meeting features, only when used: audio and transcripts of the calls and meetings you seat Vera in, including participant names
Your uploaded documents: whatever personal data your contracts contain, under your control; the service requests no special-category data
No government identifiers, no payment card data, no home addresses, no biometrics, no behavioral advertising profiles. Annex 1 of the data processing addendum (https://www.vendorbenchmark.com/dpa) states the categories of data subjects and personal data in the processor's terms.

5.3 How do file downloads work?

Every download uses a signed URL minted per authorized request, expiring after roughly 60 seconds, and never pre-signed into HTML. A leaked link or a saved page is dead before it can be abused. There are no public or long-lived links to any customer file, and every download lands in the audit log.

5.4 How long do you retain our data?

As long as you need the service, and no longer. Organization owners set a retention policy under Settings, Data controls, and the same screen shows the whole lifecycle: collected, isolated, retained on your policy, deleted on request.

5.5 What happens when we delete a contract?

The database rows and the stored files are both removed. Deletion is a data path built into the product, not a support ticket. Every contract deletion also writes a durable, timestamped deletion certificate your organization can download and keep for its own records.

5.6 What happens when we delete our whole organization?

Every storage bucket belonging to the organization is swept along with the database rows, and the deletion writes the same durable, timestamped certificate. Nothing waits in a queue for a human to action.

5.7 Can we export everything we have put in, including the files?

Yes. Organization owners export the organization's data from the data controls screen without a support ticket, and the export includes the file bytes through 1-hour signed links, not just the rows that describe them. The audit log has its own full CSV export.

5.8 What happens at the end of our contract with you?

Export, then deletion, in that order and on your initiative: owners pull the complete export including files, request full deletion, and the rows and files are removed with a deletion certificate to prove it. Your data does not linger because leaving was inconvenient to us.

6. AI AND MODEL DATA FLOW

6.1 When does AI touch our documents?

At two points. When a document is uploaded it is read once, automatically, to index it for search and to fill in its key terms: dates, values, notice periods. Everything after that, a benchmark, a brief, a question, a call, runs only when a member of your organization starts it. No training job reads your documents at any point.

6.2 What exactly leaves your platform, and to whom?

Only what a feature needs, and only to the provider that runs it.

Anthropic (Claude): the document text and the question for every written analysis, called from our servers only
Voyage AI: document text in passages, to build the search index, and the search questions
OpenAI: audio, transcripts and the deal facts Vera looks up, when you use her voice on a call or in a meeting
ElevenLabs, Recall.ai, HeyGen: call audio, meeting audio and Vera's spoken audio, only for the call copilot, the meeting seat and the video face
A live voice session streams audio from your browser to the voice model, and the browser never holds a provider credential. Nothing goes to an ad network or a third-party analytics service. Results come back to your tenant under the same row-level security as the document they came from. The full list with roles is on the subprocessor page (https://www.vendorbenchmark.com/subprocessors).

6.3 Is our data used to train AI models?

Not by us, ever, and not by the model providers that run the analysis and the voice: Anthropic and OpenAI do not use API data to train models. The zero-data-retention addendum with Anthropic is signed. The remaining providers, for search embeddings, transcription and the meeting seat, are listed with the data each one receives on the subprocessor page (https://www.vendorbenchmark.com/subprocessors).

6.4 Are AI prompts and outputs logged and attributable?

Every AI run is metered and attributable to the user and organization that ran it, so your admins can see who analyzed what. Outputs are stored in your tenant under the same row-level security as the source data.

6.5 How do we know an AI answer is grounded and not invented?

Figures in AI-generated reports are grounded in your stored data and citation tagged, and AI reports pass a groundedness check before they reach you. Curated analyst reports are verified by hand. When the assistant cites a clause, the citation points at your actual document.

7. BENCHMARKS AND DATA ANONYMITY

7.1 What goes into the benchmark pool from our contracts?

Anonymized aggregates only, and the pooling is one-way: market low, median, high and percentile positions come out, but nothing goes in attached to a name. Nothing that could identify your company, your contract or your specific terms is exposed to another customer.

7.2 Could another customer identify us from a benchmark?

No. Benchmark output is pooled and anonymized before any other customer sees it. What other customers see is the market shape: ranges and percentiles, never a data point traceable to a company, a contract or a set of terms.

7.3 Is our pricing visible to other customers?

Never in identifiable form. Your pricing contributes to pooled, anonymized aggregates, and only those aggregates are visible to anyone outside your organization.

8. INTEGRATIONS AND API

8.1 How are integration and connector credentials stored?

Encrypted at rest with AES-256-GCM, scoped to your organization, and used only server-side. No connector credential is ever sent to a browser.

8.2 How is inbound email and webhook traffic authenticated?

Inbound email and webhooks verify HMAC signatures before anything is processed, and each organization's inbound email addresses carry unguessable capability tokens, so mail sent to yours can only land in your workspace. A forged or misdirected message is uploaded, not filed.

8.3 Are your outbound webhooks signed?

Yes. Events we send you are HMAC-signed with timestamps, so your systems can verify us the same way we verify inbound traffic, and replayed payloads are detectable.

8.4 How is the API rate limited?

Per user, per IP and per API key, and in production the limiter fails closed: if the rate-limiting backend is unreachable, requests are refused rather than waved through. Authentication, upload and AI routes carry their own limits.

9. MONITORING, AUDIT AND INCIDENT RESPONSE

9.1 What does an audit event contain?

Actor, action, entity, organization, IP address and user agent, written for every view, download, create, update and delete of contract data. Reads are logged, not just writes: a view of a contract file is an audit event.

9.2 Is VendorBenchmark staff access logged too?

Identically. Analyst views and downloads of your files flow through the same audit logging as your own members' actions, in the same trail your owners can inspect and export. Staff access is never quiet access.

9.3 Can we export the audit history?

Yes. Organization owners export the complete audit history as CSV at any time, without a support ticket.

9.4 Can we stream audit events to our SIEM?

Yes. Subscribe an audit webhook and signed batches of audit events arrive every 15 minutes, cursor-tracked so nothing is skipped and a missed delivery resumes where it left off. Setup lives in the in-app Security Center.

9.5 Do you detect and alert on unusual activity?

An hourly anomaly detector reads the audit trail and emails your organization owners when one account's downloads, exports or permission changes look unusual. It runs on our side, so it works even if you never wire up the SIEM stream.

9.6 What is the Security Center?

A live posture page inside the app under Settings, Security, Posture. It exists so your team can verify the claims on these pages against your own tenant instead of taking our word for them.

MFA coverage: your organization's second-factor coverage, member by member
Audit export: the complete audit history as CSV
SIEM webhook: the signed 15-minute audit stream, set up here

9.7 Have you had a breach, and what is your incident commitment?

No customer data breach to date. The commitment if that ever changes: you hear it from us directly within 72 hours of us confirming an incident that affects your data, followed by a written post-mortem, and the audit trail shows exactly what was touched. Short-lived file links and per-request access bound the blast radius by design.

10. INFRASTRUCTURE AND SUBPROCESSORS

10.1 Where does the platform run, and how is the edge hardened?

The application runs on Vercel and the data lives in Supabase, Postgres for records and private buckets for files. Both providers are SOC 2 Type II audited. Every response carries HSTS, nosniff, frame-deny and a strict Content-Security-Policy with a fresh per-request nonce, and no secret is ever stored in the codebase; keys live in server-side environment variables only.

10.2 Where is our data located?

In the United States, all of it, today. EU data residency is not built; it sits in the Not yet column of the claim ladder rather than in a footnote.

10.3 How is data encrypted, and who manages the keys?

TLS for everything in transit. At rest, the database and storage are encrypted by our infrastructure provider, and the keys are provider-managed. We do not offer customer-managed keys (BYOK) yet, and we say so rather than blurring the line.

10.4 Who are your subprocessors, and where do we track changes?

11, each with one job.

Supabase: Postgres and file storage
Vercel: application hosting
Anthropic: document analysis and written AI answers
OpenAI: voice, transcription and live market lookups
Voyage AI: document search embeddings
Recall.ai: the meeting seat
ElevenLabs: live call transcription
HeyGen (LiveAvatar): the optional video face
Cloudflare: meeting audio relay and the public site
Resend: transactional email
Upstash: rate limiting and a short-lived cache

The current list with purpose, data and region always lives on the subprocessor page (https://www.vendorbenchmark.com/subprocessors); we notify customers before adding a provider that touches contract data.

10.5 What is your backup posture?

Provider backups are enabled on the database and storage, with continuous backup and daily snapshots, and a second, independent backup copy runs alongside them. The first restore from backup has been completed, so the backups are exercised and not only enabled, and the recovery objectives, RPO and RTO both under 24 hours, are in place. Restore tests run quarterly, and the record is in the trust center's evidence table.

11. COMPLIANCE AND LEGAL

11.1 What certifications do you hold?

None issued to VendorBenchmark yet, and we say so rather than borrowing a badge. What exists today:

SOC 2: Type I targeted Q4 2026, Type II after the observation window; the controls are implemented and mapped to evidence, and the report goes into the NDA document room when the auditor issues it
Infrastructure: Supabase (database and storage) and Vercel (hosting) are SOC 2 Type II audited; their reports are available from them
Independent validation: the first third-party penetration test is complete, annual from here; the executive summary is in the NDA document room
ISO 27001: not started; sequenced after SOC 2

The trust center (https://www.vendorbenchmark.com/trust-center) carries the dated status of each, and moves an item only when the report exists.

11.2 Where are your Master Subscription Agreement and the other agreements?

Public, on the agreements page (https://www.vendorbenchmark.com/legal), so legal can read them before anyone signs anything.

Master Subscription Agreement: the commercial terms every subscription sits under (PDF (https://www.vendorbenchmark.com/legal/master-subscription-agreement.pdf))
Data processing addendum: the processor terms, with the annexes and standard contractual clauses (PDF (https://www.vendorbenchmark.com/legal/data-processing-addendum.pdf))
Service level agreement: availability, support response and credits (PDF (https://www.vendorbenchmark.com/legal/service-level-agreement.pdf))
Acceptable use policy: what the service may and may not be used for (PDF (https://www.vendorbenchmark.com/legal/acceptable-use-policy.pdf))
Mutual NDA: for the security review itself; we sign yours or bring ours (PDF (https://www.vendorbenchmark.com/legal/mutual-nda.pdf))
Order form: the template an order is written on (PDF (https://www.vendorbenchmark.com/legal/order-form.pdf))
The executed copies come from your account team; to run the agreements through your own paper or redlines, email info@vendorbenchmark.com.

11.3 What is your SOC 2 status?

SOC 2 Type II controls are implemented and mapped to evidence, evidence collection is underway, and the report will be available under NDA when the auditor issues it. We do not claim SOC 2 until there is a report to show.

11.4 Where are you on GDPR and CCPA?

GDPR: the DPA is public at /dpa (https://www.vendorbenchmark.com/dpa), the subprocessor list at /subprocessors (https://www.vendorbenchmark.com/subprocessors), and deletion is a live product path; the records of processing are being finalized with counsel
CCPA: the privacy notice is live, and we do not sell personal data

11.5 How do we execute your DPA?

Read the standard DPA at /dpa (https://www.vendorbenchmark.com/dpa), public rather than gated behind sales, and download the addendum as a PDF (https://www.vendorbenchmark.com/legal/data-processing-addendum.pdf). To execute it, email info@vendorbenchmark.com and we complete signature as part of your procurement, on our paper or through your process.

11.6 How do we get your policies and questionnaire answers?

Through the NDA document room: request access on the trust center (https://www.vendorbenchmark.com/trust-center#request).

The links: token-scoped, gated by an NDA click-through, and every open is audit-logged
Inside: the policy set, a pre-completed security questionnaire, the penetration test summary, and the SOC 2 report when it is issued

11.7 How do we report a vulnerability?

Through the responsible disclosure policy (https://www.vendorbenchmark.com/security-disclosure), referenced from our security.txt.

Acknowledgment: within 3 business days
Good-faith research: gets safe harbor
Security is owned by: Fredrik Filipsson, founder, reachable at info@vendorbenchmark.com

11.8 Do you have a third-party penetration test?

Yes. The first independent penetration test has been completed, and the cadence from here is annual. The executive summary is available under NDA through the document room, where every open is logged. Between tests, the standing controls are the CI isolation suites and the public disclosure program with safe harbor.

11.9 How do you handle law enforcement and government requests?

We require valid legal process before disclosing customer data, and we notify the affected customer unless we are legally barred from doing so. We do not volunteer customer data, and we interpret requests narrowly.

12. PEOPLE AND PROCESS

12.1 Who at VendorBenchmark can access our contracts?

The analysts who produce your deliverables, for that purpose. Their access runs through the same audited paths as yours: every analyst view and download is logged with the person, the action, the time, the IP and the user agent, in the trail your owners can inspect and export. MFA is mandatory for every member of our staff.

12.2 How do you secure your own staff?

MFA is mandatory for every staff member, access follows least privilege, and admin actions are logged in the same audit trail as everything else. Platform admin status lives in a separate table that no customer-facing code path can write to, so it is granted deliberately, never inherited or self-assigned.

12.3 How do you secure your development process?

39 cross-tenant isolation suites run in CI on every change, so an isolation regression cannot ship quietly. Changes go through code review, and no secret is stored in the repository; keys live in server-side environment variables only.

12.4 What guards external sharing of reports?

Sharing outside your organization is an explicit action by someone in your organization, never a default. Anything shared externally passes a confidentiality scan for sensitive terms first, and external share links expire on their own.

13. WHAT WE DO NOT HAVE YET

13.1 Are you ISO 27001 certified?

No, and we have not started. SOC 2 Type II comes first; ISO 27001 is sequenced behind it.

13.2 Do you support customer-managed keys (BYOK)?

Not built. Encryption at rest is provider-managed today. If BYOK is a hard requirement for you, tell us; it is exactly the kind of signal that reorders a roadmap.

13.3 Do you offer EU data residency?

Not built. All data is hosted in the US today, and we would rather you plan on that than discover it in a data-flow diagram later.

13.4 Do you support passkeys or WebAuthn?

Not built. TOTP is the second factor today, with step-up enforcement and org-wide policy. Passkeys are on the same honest Not yet list as everything else we have not shipped.

14. THE CLAIM LADDER

Items move left only when the code or the evidence exists. The third column is there so the first can be believed.

STATUS	CONTROL OR PROGRAM	WHERE IT STANDS
Implemented	**Database-enforced tenant isolation**	Since day one, tested in CI on every change
Implemented	**TOTP MFA, step-up, org-wide enforcement**	Mandatory for our own staff
Implemented	**Enforced SSO and SCIM 2.0**	Require SSO refuses password sign-in
Implemented	**Session list, revoke, sign out everywhere**	With new-device email alerts
Implemented	**12+ character passwords, breach-screened**	Privacy-preserving check before acceptance
Implemented	**API key and SCIM token expiry**	One year maximum, hashed at rest
Implemented	**SIEM audit streaming and CSV export**	Signed 15-minute batches
Implemented	**Deletion that sweeps rows and files**	Organization deletion clears every bucket
Implemented	**security.txt and disclosure policy**	With a 3-business-day acknowledgment
Implemented	**DPA, subprocessor list and terms**	Public, no NDA needed to read them
Implemented	**AI runs in your audit trail**	Every AI run lands in your audit log with actor, feature and model
Implemented	**Privileged data paths under review ratchet**	A new code path that bypasses row-level security fails CI until reviewed
Implemented	**Break-glass sign-ins are audit-visible**	An owner using the SSO bypass writes an audit event
Implemented	**Per-org IP allowlist and session policy**	Owner-set CIDR allowlist, maximum session age and idle timeout
Implemented	**Deletion certificates**	Every contract, retention and organization deletion writes a timestamped certificate
Implemented	**Anthropic zero-retention addendum**	Signed; API data was already excluded from model training
Implemented	**Third-party penetration test**	First test completed, annual cadence
Implemented	**Backup restore test**	First restore from backup completed, quarterly from here
In progress	**SOC 2**	Type I targeted Q4 2026, Type II after the observation window; report under NDA when issued
In progress	**GDPR program**	DPA, subprocessors and deletion live; records of processing being finalized with counsel
In progress	**CCPA / CPRA**	Privacy notice live; no sale of personal data
Not yet	**ISO 27001**	Not started; SOC 2 comes first
Not yet	**Customer-managed keys (BYOK)**	Not built
Not yet	**EU data residency**	Not built; all data is hosted in the US today
Not yet	**Passkeys / WebAuthn**	Not built; TOTP is the second factor today
Not yet	**Self-serve SAML onboarding**	SSO works per organization today; fully self-serve identity provider setup is not built

15. RESILIENCE AND INDEPENDENT VALIDATION

A backup without a tested restore is a hope, and a security page without third-party validation is a promise. This table states what has happened, with dates where they exist; targets are labeled as targets. Last updated July 2026.

PROGRAM	STATUS	DETAIL
Backups	**Enabled, provider-managed, plus an independent duplicate**	Continuous backups with daily snapshots on Supabase (SOC 2 Type II audited), and a second, independent backup copy running alongside them. A backup is a hope until a restore proves it, which is what the restore test below is for.
Backup restore test	**First test completed**	Quarterly program. The first restore from backup has been completed; each run is recorded here.
Recovery objectives	**In place: RPO under 24 hours, RTO under 24 hours**	In place and exercised by the restore test above; each quarterly run is recorded here with the measured result.
Third-party penetration test	**First test completed**	Annual cadence. The executive summary is available in the NDA document room; every access is logged.
SOC 2	**Type I targeted Q4 2026**	Controls implemented and mapped to evidence today; Type II follows after the observation window. The report lands in the NDA document room when the auditor issues it.

16. CERTIFICATIONS AND ATTESTATIONS

The question every IT security review asks first, answered without a borrowed badge.

CERTIFICATION OR ATTESTATION	STATUS	DETAIL
Certifications held by VendorBenchmark	**None issued yet**	We do not borrow a badge: no certification is claimed until a report exists.
SOC 2	**Type I targeted Q4 2026**	Controls implemented and mapped to evidence; Type II after the observation window; report in the NDA document room when issued.
Infrastructure providers	**SOC 2 Type II audited**	Supabase (database and storage) and Vercel (hosting); their reports are available from them.
Independent validation	**Penetration test completed**	First third-party test complete, annual cadence; the executive summary is in the NDA document room.
ISO 27001	**Not started**	Sequenced after SOC 2.

17. WHAT WE COLLECT ABOUT INDIVIDUALS

For your authorized users: name, work email, the timezone they set, and the sign-in credential (a password hash, or nothing when you use SSO). Beyond that, the platform records only what operating it securely requires, and nothing for marketing or profiling.

DATA	WHAT AND WHY
Audit and session records	The IP address, user agent and time of each sign-in and each action on contract data, and the devices a user is signed in on, kept so your owners can inspect the trail
Activity attribution	Which user ran which benchmark, AI analysis or export, in your own tenant
Voice and meeting features, only when used	Audio and transcripts of the calls and meetings you seat Vera in, including participant names
Your uploaded documents	Whatever personal data your contracts contain, under your control; the service requests no special-category data

No government identifiers, no payment card data, no home addresses, no biometrics, no behavioral advertising profiles. Annex 1 of the data processing addendum, later in this guide, states the categories of data subjects and personal data in the processor's terms.

18. THE AGREEMENTS

Every agreement is public as a PDF at https://www.vendorbenchmark.com/legal, so legal can read the terms before anyone signs; the executed copies come from your account team, and the agreements can run through your own paper or redlines on request to info@vendorbenchmark.com.

AGREEMENT	WHAT IT COVERS	WHERE
Master Subscription Agreement	The commercial terms every subscription sits under: license, fees, confidentiality, warranties, liability, term and termination.	https://www.vendorbenchmark.com/legal/master-subscription-agreement.pdf
Data processing addendum	The processor terms, with the annexes and the standard contractual clauses where a transfer requires them.	https://www.vendorbenchmark.com/legal/data-processing-addendum.pdf
Service level agreement	Availability, support response and service credits.	https://www.vendorbenchmark.com/legal/service-level-agreement.pdf
Acceptable use policy	What the service may and may not be used for.	https://www.vendorbenchmark.com/legal/acceptable-use-policy.pdf
Mutual NDA	For the security review itself; we sign yours or bring ours.	https://www.vendorbenchmark.com/legal/mutual-nda.pdf
Order form	The template an order is written on.	https://www.vendorbenchmark.com/legal/order-form.pdf

19. FRAMEWORK STATUS

FRAMEWORK	SCOPE	STATUS	WHERE WE STAND
SOC 2 Type II	Security, Availability and Confidentiality criteria	**In progress**	The technical controls an auditor tests are already implemented. We are formalizing the policy set and evidence collection ahead of the observation window. We will not describe the platform as SOC 2 attested until a report exists, which we will share under NDA.
GDPR	For customers with EU and EEA data subjects	**In progress**	A data processing addendum is available, subprocessors are published, and customer-initiated deletion removes both rows and files. Records of processing and the data subject request workflow are being finalized with counsel before we describe the platform as GDPR compliant.
CCPA / CPRA	For California consumers and business contacts	**In progress**	Our privacy notice sets out the categories collected, purposes and consumer rights. We do not sell personal information. The rights intake and service-provider terms are being confirmed with counsel before we describe the platform as CCPA compliant.
ISO 27001	Information security management	**Planned**	Not started. SOC 2 comes first; ISO 27001 is sequenced behind it.

SOC 2 is an attestation issued by a licensed CPA firm after an audit, not a self-declared status. GDPR and CCPA have no government certification. VendorBenchmark describes a framework as satisfied only when it can show the evidence.

20. THE AI DATA FLOW

Written the way a data processing answer is written: when a document is read, what leaves the platform, to whom, what comes back, and how it is retained and attributed.

1. **Read once on upload, then only when you act.** An uploaded document is read once, automatically, to index it for search and fill in its key terms. Every analysis after that runs only when a member of your organization starts it. No training job reads your documents.
2. **What leaves, and to whom.** Written analysis goes to Anthropic (Claude). Document passages for search go to Voyage AI. Call and meeting audio goes to OpenAI and the voice providers, only when you use Vera's voice. Nothing goes to an ad network or a third-party analytics service; every provider is on the subprocessor list.
3. **What comes back, and where it lives.** The analysis returns to your tenant and is stored under the same row-level security as the document it came from.
4. **Retention and training.** Anthropic and OpenAI do not use API data to train models, and the zero-data-retention addendum with Anthropic is signed.
5. **Attribution.** Every AI run is metered and attributable to the user and organization that ran it, so your admins can see who analyzed what.

21. SUBPROCESSORS

The complete list of third parties that touch the service, with the purpose of each, the data it receives and where it processes it. A provider is listed when production sends it customer data; at least thirty days notice is given before a

provider that touches contract data is added or replaced. OpenAI, Recall.ai, ElevenLabs, HeyGen (LiveAvatar) and Cloudflare's audio relay are on the path only for the voice, call and meeting features; a workspace that never uses them sends them nothing. Last updated October 1, 2026.

SUBPROCESSOR	PURPOSE	DATA TOUCHED	LOCATION
Supabase	Database and private file storage (Postgres, storage buckets), encrypted at rest	Contract documents, application data	United States
Vercel	Application hosting and edge network	Application traffic	United States
Anthropic	AI model API (Claude), called server side for document analysis and every written AI answer; API data is not used to train models	Contract text and questions sent for AI features; larger documents are held as files on our Anthropic account so they are not re-sent on every turn	United States
OpenAI	Vera's voice on calls and in meetings, speech to text, text read aloud, and the public web lookup she runs during a call	Audio from the calls and meetings where you use the voice features, their transcripts, the text read aloud, and the deal facts Vera looks up to answer	United States
Voyage AI	Embeddings that power document search	Contract text, split into passages when a document is indexed, and the search questions asked against it	United States
Recall.ai	The meeting participant that joins a Zoom, Teams or Meet call when you seat Vera in it	Audio and transcript, with participant names, of the meetings you seat Vera in	United States
ElevenLabs	Speech to text for the live call copilot, and the vendor's voice in negotiation rehearsal	Audio segments from calls where the copilot is listening, and rehearsal lines	United States
HeyGen (LiveAvatar)	Renders the optional video face while Vera speaks	The audio of Vera's spoken answers; no microphone audio and no documents	United States
Cloudflare	Relays meeting audio between the meeting seat and the voice model, and serves the marketing site and the public contract decoder	Meeting audio in transit for meetings where Vera is seated, and decoder traffic in transit	Global edge
Resend	Transactional email delivery, and receiving the email you forward in	Recipient name and email, notification content, forwarded messages	United States
Upstash	Rate limiting and a short-lived cache (Redis)	Request counters keyed by user or IP, and cached AI results that expire on a timer	United States

22. SHARED RESPONSIBILITY

WHAT VENDORBENCHMARK RUNS	WHAT OUR INFRASTRUCTURE RUNS	WHAT YOU CONTROL
The platform and its controls.	SOC 2 Type II audited providers, listed with roles on the subprocessor page.	The controls only your organization can turn.

WHAT VENDORBENCHMARK RUNS	WHAT OUR INFRASTRUCTURE RUNS	WHAT YOU CONTROL
• Tenant isolation policies and their CI test suites • Application access control, MFA step-up, SSO enforcement • Audit logging, SIEM streaming and security alerting • Upload validation and short-lived signed downloads • Secret handling, key hashing and connector encryption • Incident response for the platform, with direct customer notification	• Supabase: Postgres hosting, storage, encryption at rest, backups • Vercel: application hosting, TLS termination, edge network • Anthropic: AI model inference, no training on API data • OpenAI: voice and transcription, no training on API data • Provider status pages: status.supabase.com and vercel-status.com	• Enforce MFA or Require SSO for your organization • Review members, roles and per-contract access regularly • Rotate API keys and SCIM tokens; they expire within a year regardless • Subscribe the audit stream to your SIEM and watch it • Delete contracts and data you no longer need us to hold

23. THE DATA PROCESSING ADDENDUM, CLAUSE BY CLAUSE

The addendum (VB-DPA, version 1.0, effective July 2026) forms part of the Master Subscription Agreement and applies where VendorBenchmark LLC processes personal data on the customer's behalf. The addendum itself governs; the summary below follows its own numbering. The document is public at https://www.vendorbenchmark.com/legal/data-processing-addendum.pdf, and the executed copy comes from your account team.

1. **Roles and scope.** For the personal data in your customer data, you are the controller and VendorBenchmark LLC is the processor, for the term of the agreement and until the data is deleted or returned. Where you act as a processor for a third-party controller, the addendum applies with you as processor and us as sub-processor, and that controller's instructions reach us through you.
2. **Processing instructions.** We process personal data only on your documented instructions: the agreement, the addendum and the way you configure the service. We tell you if an instruction appears to infringe data protection law and may pause that processing until it is confirmed or withdrawn. We do not sell personal data and process it for no purpose other than providing and supporting the service.
3. **Confidentiality of personnel.** Everyone we authorize to process personal data is bound by confidentiality obligations, trained on their data protection responsibilities, and given access only as needed, under least privilege.
4. **Security measures.** We implement the technical and organizational measures in Annex 2: tenant isolation enforced at the database, encryption in transit and at rest, least-privilege access with multi-factor authentication, audit logging of views and downloads, private file storage behind short-lived signed URLs, secure development, encrypted backups with tested restoration, and personnel measures. We may update them, never materially reducing the level of protection during the term. The full architecture is on the security overview (https://www.vendorbenchmark.com/security).
5. **Subprocessing.** You give general authorization for the subprocessors on the subprocessor list (https://www.vendorbenchmark.com/subprocessors). We give at least thirty days notice before adding or replacing one; you may object on reasonable data protection grounds, and if the objection cannot be resolved you may terminate the affected part of the service with a refund of prepaid unused fees. Every subprocessor is bound by written obligations no less protective than the addendum, and we remain fully liable for their performance.
6. **Data subject requests.** We assist you, with appropriate technical and organizational measures, in responding to data subjects exercising their rights. A request made directly to us is referred to you unless the law requires otherwise.
7. **Assistance.** Taking into account the nature of the processing, we assist you with the security of processing, personal data breaches, data protection impact assessments and prior consultation with supervisory authorities.

8. **Personal data breach.** We notify you without undue delay after becoming aware of a personal data breach affecting your personal data, with the nature of the breach, the categories and approximate number of data subjects and records, the likely consequences and the measures taken, supported by the audit trail that shows what was accessed. Our standing commitment is that you hear it from us within 72 hours of confirmation.
9. **International transfers.** All data is hosted in the United States today. Where a transfer reaches a country without an adequacy decision, the applicable standard contractual clauses are incorporated by reference and completed by the annexes, with the United Kingdom or Swiss addendum where that regime applies. The clauses prevail over the addendum for the transfers they govern.
10. **Government and third-party access.** If a public authority makes a legally binding request for your personal data, we notify you before responding unless the law prohibits it, review the legality of each request, challenge requests we consider unlawful or overbroad, and disclose only the minimum required.
11. **Deletion and return.** On termination, and on your request at any time, we delete or return your personal data at your direction, using the platform's hard-delete path that removes both the database rows and the stored files and writes a deletion certificate. Unless you direct otherwise, deletion follows within ninety days of termination, except where the law requires retention, and then only for as long as it requires.
12. **Audits.** We make available the information reasonably necessary to demonstrate compliance, including third-party certifications and audit reports where available, and allow audits by you or an auditor you mandate on reasonable notice, once in any twelve-month period unless a supervisory authority or a breach requires more, during business hours and without compromising other customers' data.
13. **Liability and precedence.** Each party's liability under the addendum is subject to the limitations in the agreement. On data protection, the addendum prevails over the agreement, and the standard contractual clauses prevail over both for the transfers they govern.
14. **The signed addendum.** This page is a summary. The addendum itself, with the annexes and the standard contractual clauses where they apply, is at /legal/data-processing-addendum.pdf (https://www.vendorbenchmark.com/legal/data-processing-addendum.pdf). To execute it, email info@vendorbenchmark.com or your account team, and we complete signature as part of your procurement, on our paper or through your process.

Annex 1, details of processing.

ITEM	DETAIL
Roles	Customer is controller (or processor for a third-party controller); Provider is processor (or sub-processor)
Subject matter	Provision of the Vera AI contract benchmarking and vendor-spend platform
Duration	The term of the agreement, plus the retention and deletion periods it sets
Nature and purpose	Hosting, processing and analysis of customer data to produce benchmarks and deliverables and to operate the accounts
Categories of data subjects	The customer's personnel who are authorized users, and individuals named in the customer's uploaded documents
Categories of personal data	Names and business contact details of authorized users, and any personal data the customer includes in uploaded documents
Special categories	None requested by the service; the customer controls and should avoid uploading special-category data

ITEM	DETAIL
Frequency	Continuous for the duration of the agreement

Annex 2, technical and organizational measures.

a. Tenant isolation enforced at the database with row-level security, so a session from one organization cannot return another organization's rows

b. Encryption of personal data in transit with TLS and at rest

c. Access control with least privilege, role-based access, multi-factor authentication available to all users and mandatory for provider staff, and short session lifetimes

d. Audit logging of who did what to which contract and when, including views and downloads of contract files

e. Storage of contract files in private buckets, accessed only through short-lived signed URLs, never public URLs

f. Secure development with code review, dependency management and environment separation, and secrets held only in server-side configuration

g. Resilience through encrypted backups, tested restoration, and monitoring with alerting

h. Personnel measures including confidentiality obligations, security training, and least-privilege provisioning and deprovisioning

24. RESPONSIBLE DISCLOSURE

How to report. Email info@vendorbenchmark.com with the subject line “Security report”. Include what you found, the steps to reproduce it, the url or endpoint involved, the impact you believe it has. A proof of concept helps; access to another customer's data does not need to be proven beyond the first record.

What VendorBenchmark commits to. We acknowledge reports within 3 business days; We keep you informed while we investigate, and tell you when the issue is fixed; We do not run a paid bounty program today; We credit researchers who want credit, and we say thank you properly.

Safe harbor. We will not pursue legal action for research that stays within this policy. The terms: act in good faith; access only what is needed to demonstrate the issue; do not read or modify other customers' data beyond the minimum proof; do not degrade the service; give us reasonable time to fix the issue before any public disclosure.

Out of scope. Denial of service and volumetric testing; Social engineering of our staff or customers; Physical attacks and attacks on third-party services we use; Reports from automated scanners without a demonstrated impact.

The machine-readable policy is the RFC 9116 security.txt at https://app.vendorbenchmark.com/.well-known/security.txt. Security at VendorBenchmark is owned by Fredrik Filipsson, founder, at info@vendorbenchmark.com.

25. HOW TO RUN THE REVIEW

1. **Read in order.** The security overview, the questions in this guide, the addendum, the subprocessor list, the terms, the trust center and the disclosure policy: roughly ninety minutes, no account needed.
2. **Verify three things alone, in a trial tenant.** Create two organizations, upload a document to one and confirm the other's session cannot read it, the denial coming from the database; subscribe an audit webhook and watch signed, cursor-tracked batches of your own events arrive within 15 minutes; delete a contract, confirm rows and files are gone, and download the deletion certificate the deletion wrote.

3. **Request the NDA document room.** For the pre-completed security questionnaire, the penetration test executive summary, the policy set and the SOC 2 report when issued, at https://www.vendorbenchmark.com/trust-center.
4. **Send your questionnaire as it is.** To info@vendorbenchmark.com; VendorBenchmark completes it in your format, walks the architecture with your team, and demonstrates the cross-tenant access attempt failing live.
5. **Execute the addendum.** On our paper or through your process, as part of procurement, with the standard contractual clauses where a transfer requires them.

VendorBenchmark LLC
1007 N Orange St, 4th Floor, Suite #5951, Wilmington, Delaware 19801, United States
info@vendorbenchmark.com |
https://www.vendorbenchmark.com

This guide describes the platform as of July 2026. The web pages named above are kept current and govern where they and this file disagree. It is not the signed agreement; the executed addendum and terms are provided by your account team.