

BoardCue Live Subprocessor and Data Flow Register

Last updated: 2 October 2026

Status: Verified facts plus clearly marked vendor-confirmation points

Current cloud AI processing architecture

BoardCue sends authorised cloud AI requests directly to the Google Gemini Developer API (<https://generativelanguage.googleapis.com>) and OpenAI API (<https://api.openai.com>), using server-held credentials and server-selected models. No Lovable intermediary AI gateway is used in this processing path. The Google service is the Gemini Developer API, not Vertex AI.

Requests using /v1/chat/completions, including product analysis, summaries, minutes, questions, public/support chat and PDF OCR, may make at most 1 alternate-provider attempt when the alternate credential is configured. Failover is permitted for HTTP 401, 402, 403, 404, 429, errors marked retryable by the transport (including HTTP 500 and above, network/read errors, timeouts and unexpected native PDF response-normalisation errors), missing primary credentials or unreadable JSON responses. The original messages, retrieved context and attachments can therefore reach both providers during one logical request; model and provider-specific options are adapted. Input validation, size-limit failures and other non-retryable failures do not trigger failover. This does not guarantee that the alternate provider accepts every payload.

Embeddings do not fail over: product embeddings use Google's gemini-embedding-001 with 3,072 dimensions and response validation. Google PDF OCR sends inline PDF page data to the native generateContent endpoint; it does not upload to a Files API, but remains eligible for chat-path failover. Response parsing after the transport has returned does not itself trigger provider failover. Standard live speech recognition uses the browser/OS speech service, not this cloud AI transport. Local-browser AI is rejected by the server adapter and has no cloud fallback.

The repository establishes API routing, not the supplier account's contractual status. The applicable Google Gemini Developer API and OpenAI API account terms, billing/service tier, DPA and transfer safeguards, processing geography, content-use/training settings, logging and retention must be verified and recorded by the supplier-assurance owner. No zero-retention, UK-only or specific regional AI processing, Google Cloud enterprise controls, enhanced OpenAI retention terms or special contractual arrangement is asserted here.

Register date: 30 August 2026

1. Publication principles

This register distinguishes BoardCue production facts from supplier-published facts and from items that remain unverified. A generic supplier capability is not presented as though it were the actual BoardCue configuration.

2. Current supplier register

Supabase

Purpose: Authentication, database and document storage

Data: Account data, Customer Content, audit/security data

BoardCue status: Production Supabase primary database and document storage: United Kingdom. Enterprise go-live: Pro or higher.

Published/assurance position: Supabase DPA/transfer controls; Pro daily database backups with current published 7-day access window.

Open action: Verify Pro upgrade and Backups screen at enterprise go-live.

Google Gemini Developer API

Purpose: Primary cloud AI and embeddings for selected governance tasks

Data: Prompts, retrieved source context, outputs, embeddings and associated request metadata

BoardCue status: Direct Gemini Developer API using a server-held API key; no intermediary AI gateway.

Published/assurance position: The repository establishes API routing, not the supplier account's contractual status. The applicable Google Gemini Developer API and OpenAI API account terms, billing/service tier, DPA and transfer safeguards, processing geography, content-use/training settings, logging and retention must be verified and recorded by the supplier-assurance owner. No zero-retention, UK-only or specific regional AI processing, Google Cloud enterprise controls, enhanced OpenAI retention terms or special contractual arrangement is asserted here.

Open action: Human verification required: retain evidence of the actual Gemini Developer API account terms and settings.

OpenAI API

Purpose: Selected cloud AI analysis and alternate-provider chat/PDF OCR attempts

Data: Prompts, retrieved source context, outputs, attachments and request metadata, including eligible failover requests

BoardCue status: Direct ADEPTABLE-controlled API account, with no intermediary AI gateway.

Published/assurance position: The repository establishes API routing, not the supplier account's contractual status. The applicable Google Gemini Developer API and OpenAI API account terms, billing/service tier, DPA and transfer safeguards, processing geography, content-use/training settings, logging and retention must be verified and recorded by the supplier-assurance owner. No zero-retention, UK-only or specific regional AI processing, Google Cloud enterprise controls, enhanced OpenAI retention terms or special contractual arrangement is asserted here.

Open action: Human verification required: retain evidence of the actual OpenAI API account terms and retention settings; no enhanced retention is assumed.

Resend

Purpose: Outbound transactional email

Data: Recipient email, message content, delivery metadata

BoardCue status: Production use confirmed.

Published/assurance position: Supplier DPA and international-transfer safeguards apply.

Open action: Maintain annual supplier evidence.

Postmark / ActiveCampaign

Purpose: Inbound intelligence email

Data: Sender/recipient, body, headers, attachments, delivery metadata

BoardCue status: Production use confirmed.

Published/assurance position: Supplier DPA and international-transfer safeguards apply.

Open action: Maintain annual supplier evidence.

Stripe

Purpose: Payments/subscriptions

Data: Payer/account identifiers, billing/transaction data

BoardCue status: Production use confirmed. Governance Customer Content is not intentionally sent to Stripe.

Published/assurance position: Stripe DPA/data-transfer arrangements apply.

Open action: Maintain annual supplier evidence.

Malware-scanning provider

Purpose: Inbound attachment malware scan, if configured

Data: Attachment bytes

BoardCue status: Fail-closed integration exists, but no production provider is verified.

Published/assurance position: No provider named until configuration evidence exists.

Open action: Verify deployed provider before enabling relevant inbound attachment flow.

3. Browser or operating-system speech recognition

Browser/OS speech recognition is not automatically a BoardCue subprocessor. In the managed Live Board route, BoardCue invokes the speech-recognition capability available in the user's browser/device environment and receives transcript text.

The organisation is responsible for approving and configuring the browsers, operating systems and devices its users may use. ADEPTABLE does not warrant where or how a third-party browser/OS provider processes speech data.

4. Core data flows

1. User -> BoardCue -> Supabase authentication/database/storage (United Kingdom).
2. Authorised AI request -> BoardCue server -> direct Google Gemini Developer API and/or OpenAI API under ADEPTABLE-controlled accounts -> response -> BoardCue.
3. Meeting audio -> customer-selected browser/OS speech service -> transcript text -> BoardCue.
4. BoardCue notification -> Resend -> recipient.
5. Sender -> Postmark -> BoardCue inbound route -> quarantine -> configured malware scanner if present -> workspace.
6. Customer -> Stripe -> subscription/payment status -> BoardCue.

5. Public wording rules

- Do not state that all BoardCue data stays in the UK. BoardCue's primary Supabase database and document storage are hosted in the United Kingdom. Other suppliers may still process data outside the UK, so BoardCue does not claim that all processing is UK-only.
- Do not state zero retention or no model training by downstream AI providers until the direct AI provider route is confirmed end to end.
- Do not name a malware scanner as an active subprocessor until production configuration proves it.
- Do not present supplier certifications as ADEPTABLE certifications.

6. Source basis

- Supabase regions: <https://supabase.com/docs/guides/platform/regions>
- Supabase backups: <https://supabase.com/docs/guides/platform/backups>
- Resend GDPR/DPA: <https://resend.com/security/gdpr> and <https://resend.com/legal/dpa>
- Postmark EU privacy/DPA: <https://postmarkapp.com/eu-privacy> and <https://postmarkapp.com/dpa>
- Stripe DPA: <https://stripe.com/legal/dpa> and Stripe Privacy Center
- BoardCue production facts: repository audit dated 30 August 2026 and Supabase production dashboard evidence supplied by ADEPTABLE.

Meeting Effectiveness data flow

Eligible meeting participant -> seven-dimension ratings and optional comments -> organisation-scoped Supabase records -> minimum-three-response suppression and anonymous aggregation -> authorised organisation reporting. Protected participant identifiers enforce eligibility, one response per participant and the seven-day response window.