

BoardCue Live Master Product Data Protection Impact Assessment

Last updated: 2 October 2026

Status: Conditional approval for enterprise use subject to open implementation and vendor gates

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.

1. Executive decision

A full DPIA remains appropriate because BoardCue combines innovative AI, live meeting transcription, retrieval across multiple governance sources and potentially sensitive information. The assessment reflects BoardCue's governance purpose rather than treating it as an operational case-management platform. BoardCue is a corporate governance system. It is not intended to replace sector-specific operational systems, hold routine individual case-management datasets, or make operational decisions about individual people.

2. Processing assessed

- account and organisation administration;
- board and committee content storage;
- document extraction, indexing, retrieval, embeddings and search;
- AI analysis and generation directly to approved Google Gemini Developer API and OpenAI API routes;
- managed browser/OS speech transcription; the retired cloud-audio transcription route is unavailable;
- meeting preparation, live governance prompts and institutional board memory;
- actions, decisions, approvals, briefings and workflow automation;
- governance audit and export;
- outbound email via Resend, inbound email via Postmark, payment via Stripe;

- controlled support access and security/operational logging.

3. Data subjects and data sensitivity

The principal data subjects are BoardCue users, board/committee members, executives, employees/workers, meeting participants, complainants, whistleblowers, advisers and individuals referred to in governance material. People connected with an organisation's services, workforce, customers, beneficiaries or other stakeholders may be referred to incidentally in governance material, particularly in incident, safeguarding, complaint or workforce reporting. They are not intended to form routine individual case-management datasets. Organisations should use aggregated, anonymised or summarised evidence where practical.

4. Core data flows

1. Account/workspace: User -> BoardCue -> Supabase authentication/database/storage in the United Kingdom.
2. Cloud AI: Authorised BoardCue server request -> Google Gemini Developer API and/or OpenAI API under ADEPTABLE-controlled accounts -> response -> BoardCue. Enterprise deployment must verify actual processing geography, retention, content-use/training settings, account terms and transfer safeguards for each active API service; regional processing is not assumed.
3. Managed Live transcription: Meeting audio -> browser/OS speech-recognition capability selected by the user's environment -> transcript text -> BoardCue. Customer controls/approves its browser/device environment.
4. Outbound email: BoardCue -> Resend -> recipient.
5. Inbound intelligence: Sender -> Postmark -> BoardCue inbound route -> quarantine -> configured malware scanner if present -> workspace.
6. Payments: Customer -> Stripe -> payment/subscription status -> BoardCue.

5. Verified infrastructure and supplier position

Supabase Production primary database and document-storage region: United Kingdom. Enterprise go-live baseline: Pro or higher with daily backups, 7- day availability according to Supabase published documentation.

Google Gemini Developer API/OpenAI Architecture and model routes verified in code. Exact direct AI provider processing geography, retention, logging, downstream account terms and transfer controls remain pending written vendor confirmation.

Resend Production outbound service confirmed. Resend publishes US data storage, standard 30-day active-account email/log retention and UK transfer safeguards through its DPA.

Postmark Production inbound service confirmed. Postmark publishes US data storage/processing and DPA/SCC/UK Addendum arrangements.

Stripe Production payment service confirmed. Payment information is kept separate from governance Customer Content; Stripe publishes UK DPA transfer arrangements.

Malware scanning Fail-closed integration exists, but no production provider has yet been verified. Do not name a scanner as an active subprocessor until verified.

6. Necessity and proportionality controls

1. Human judgement remains responsible for governance decisions.
2. Source evidence should be distinguishable from AI interpretation.
3. Customers should not upload identifiable or sensitive data where aggregated or anonymised evidence is sufficient.
4. Role and committee access should be least-privilege and periodically reviewed.
5. Organisations are responsible for approving/configuring the browsers and endpoints used for browser speech recognition.
6. Meeting participants should be told when transcription is active and why.
7. Derived AI/search content should follow the source-data lifecycle.

- 8. Support access should be exceptional, authorised, time-limited and audited.
- 9. Organisation customers should be able to export and delete their governance record.

7. Principal risks and controls

R1

Risk: Participants unaware of transcription

Initial: High

Control: Meeting notice, host responsibility, participant notice template

Residual: Medium

R2

Risk: Browser/OS speech provider handles audio in a way the customer has not approved

Initial: High

Control: Organisation approves/configures its endpoint/browser environment; BoardCue does not warrant third-party browser processing

Residual: Medium

R3

Risk: Google Gemini Developer API/OpenAI retention/geography is insufficiently evidenced

Initial: High

Control: Supplier register; vendor questions sent; no unverified zero-retention/UK-only claim

Residual: Medium/High until response

R4

Risk: Individual-level operational case data is uploaded unnecessarily

Initial: High

Control: Intended-use restriction; guidance to use aggregated, anonymised or summarised governance evidence; customer DPIA/minimisation

Residual: Medium

R5

Risk: Sensitive workforce/incident information is overexposed

Initial: High

Control: Role/committee permissions, MFA, RLS, customer access review

Residual: Medium

R6

Risk: AI output is treated as fact

Initial: High

Control: Source-backed evidence, human review, no automatic approval

Residual: Medium

R7

Risk: Cross-organisation data leakage

Initial: Critical

Control: Tenant/RLS controls, automated tenancy testing

Residual: Low/Medium

R8

Risk: Terminated organisation data persists indefinitely

Initial: High

Control: 14-day exit/deletion design and deterministic deletion implementation in progress

Residual: Medium until implemented

R9

Risk: Backup lifecycle contradicts deletion promise

Initial: High

Control: Enterprise Supabase Pro baseline and verified backup lifecycle; deletion state reapplied after restore

Residual: Medium

R10

Risk: Data breach notification is delayed by 'confirmation' step

Initial: High

Control: Revised awareness-based notification clause; 24-hour operational target

Residual: Low/Medium

R11

Risk: MFA organisation requirement is bypassed through server operations

Initial: High

Control: Current org MFA control; server-side AAL2 hardening identified for implementation

Residual: Medium until implemented

R12

Risk: Service-level promise cannot be evidenced

Initial: Medium

Control: No contractual 99.5% commitment until health monitoring and monthly measurement are implemented

Residual: Low/Medium

8. Enterprise open actions

- Obtain direct Google Gemini Developer API and OpenAI API services written assurance and update downstream Google/OpenAI transfer assessment.
- Implement and verify the Full Organisation Exit Export, 14-day read-only closure window and deterministic deletion workflow.
- Complete server-side organisation MFA enforcement hardening.
- Implement external health/availability monitoring before activating the 99.5% SLA.
- Verify production malware-scanning provider if inbound attachments are enabled.
- Upgrade/operate enterprise deployments on Supabase Pro or higher and retain evidence of current backup settings.
- Commission independent penetration testing and pursue Cyber Essentials as part of the assurance programme.

9. Residual decision

Residual product privacy risk is assessed as Medium, with specific Medium/High uncertainty remaining for Google Gemini Developer API/OpenAI supplier terms and implementation-dependent exit/deletion controls. Marketing and controlled onboarding can proceed provided these gaps are stated accurately and are closed or accepted before the affected enterprise deployment.