

BoardCue Live Privacy Policy

Last updated: 2 October 2026

Status: Clean revised draft

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.

This Privacy Policy explains how ADEPTABLE LTD processes personal data in connection with BoardCue Live, our website, enquiries, subscriptions, support and related services. Contact: privacy@boardcue.live.

1. Controller and processor roles

ADEPTABLE is normally controller for its own account administration, billing, security, service administration, enquiries, support administration, legal/compliance records and its own marketing activities.

Where an organisation uses BoardCue for its board, committee or governance information, the organisation will normally determine why that content is processed and act as controller. ADEPTABLE will normally act as processor for Customer Content under the BoardCue Data Processing Agreement.

2. Intended data scope

BoardCue is a corporate governance platform. It is not intended as an electronic patient record, clinical record repository or direct-care clinical decision-support system.

Routine use should involve governance information such as board and committee papers, minutes, risks, strategies, performance reports, actions and decisions. Routine individual case-management datasets are outside intended use. Where governance material refers to identifiable individuals, organisations should normally use aggregated, anonymised, summarised or otherwise appropriately governed information where practical.

Sensitive personal data can still appear legitimately or incidentally in governance material, for example in workforce matters, complaints, serious incidents, safeguarding matters or whistleblowing material.

3. Personal data we process

- Account and identity information: name, email, organisation, role, authentication state, MFA status and account metadata.
- Customer Content: governance documents, board packs, minutes, transcripts, strategies, risks, actions, decisions, briefings, discussions, approvals and supporting material.
- Meeting information: meeting metadata, participants identified in meeting information, transcript text, timestamps and speaker labels where available.
- AI and search information: prompts, source extracts, responses, retrieval context, embeddings and related metadata.
- Governance workflow information: action owners, decision participants, approval or voting records, reminders, workflow events and audit information.
- Technical and security information: device/browser information, timestamps, authentication/security events, audit logs, diagnostics and IP address where processed by our infrastructure or security tools.
- Billing, enquiry and support information.

4. Sensitive information

Governance material can contain special-category, criminal-offence or otherwise highly confidential information. ADEPTABLE does not require customers to upload sensitive information merely because the product can technically process it. Customers should apply data minimisation and only use information necessary and lawful for their governance purpose.

5. Lawful bases for ADEPTABLE controller processing

Account administration

Typical basis: Contract or steps before contract

Authentication and service security

Typical basis: Contract; legitimate interests in security and fraud prevention

Billing

Typical basis: Contract; legal obligation for accounting/tax records

Support and enquiries

Typical basis: Contract/steps before contract; legitimate interests

Security and audit records

Typical basis: Legitimate interests; contract; legal obligation where applicable

Legal/compliance administration

Typical basis: Legal obligation; legitimate interests

6. AI processing

BoardCue uses cloud AI for governance analysis, questions, summaries, minutes, assurance analysis, search and embeddings. The implemented route sends authorised requests from the BoardCue server through the direct Google Gemini Developer API and OpenAI API services to approved Google or OpenAI model routes selected server-side.

ADEPTABLE does not intentionally use Customer Content to train a general-purpose model for its own independent purposes. The exact direct AI provider retention, logging, downstream provider, training/content-use and international-transfer position is subject to written vendor confirmation and is maintained in the Subprocessor Register. We do not make stronger provider-side zero-retention or data-residency claims until confirmed end to end.

7. Browser speech recognition

The managed Live Board interface can use speech recognition supplied by the user's browser, operating system or device. The third-party browser or operating-system provider determines whether recognition occurs locally or through its own remote service.

ADEPTABLE does not select or control the customer's browser, operating system or device provider and does not warrant that provider's processing location, retention or technical behaviour. Organisations are responsible for approving and configuring the endpoint environment their users are permitted to use. BoardCue receives and stores the returned transcript text according to the customer's workspace settings.

8. Email, inbound intelligence and payments

BoardCue uses Resend for outbound transactional email and Postmark for inbound intelligence email. Inbound attachments are quarantined and are only ingested where the configured malware scanning control passes. If no production malware scanner is configured, the relevant attachment-ingestion path is designed to fail closed.

Stripe processes payments and subscriptions. BoardCue receives subscription and transaction metadata needed to administer the account and does not intentionally store full payment card numbers.

9. Hosting and supplier locations

The BoardCue production Supabase project, including its primary database and document storage, is hosted in the United Kingdom. For enterprise go-live, ADEPTABLE's deployment assumption is Supabase Pro or higher. Supabase states that Pro projects receive automatic daily database backups with the last 7 days available.

Other suppliers may process or make data accessible outside the UK or EEA. The Subprocessor Register identifies verified supplier-published positions and distinguishes them from BoardCue-specific facts that remain subject to vendor confirmation.

10. International transfers

Where ADEPTABLE is responsible for a restricted transfer, it will use an applicable lawful transfer mechanism, which may include adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to EU Standard Contractual Clauses or another lawful safeguard, together with any required transfer assessment/data protection test.

11. Retention and exit

Active organisation Customer Content is retained for the customer-controlled workspace lifecycle unless the customer contract or retention configuration provides otherwise. Derived search, embedding and AI context data should follow the lifecycle of the source.

At the end of an organisation service, Customer Personal Data will be returned/exported or deleted under the Data Processing Agreement. Where the Full Organisation Exit workflow is enabled for the deployment, a complete organisation export is made available for 14 calendar days after the customer is notified that it is ready, after which active-system deletion begins unless a lawful contrary instruction or legal hold applies.

Protected backups may persist beyond active-system deletion until the ordinary backup lifecycle expires, while remaining beyond normal use. For enterprise deployments using Supabase Pro, the current baseline assumption is a 7-day daily database backup window, subject to verification at go-live.

12. Security

Controls include authenticated access, organisation-enforceable MFA, role and committee permissions, row-level data restrictions, audit logging, rate and payload limits, controlled support access, HTTPS/TLS, quarantine/fail-closed attachment handling where configured, and deletion-integrity controls as implemented.

No internet service can be guaranteed completely secure. Customers remain responsible for user access, device/browser security, information classification and appropriate meeting practice.

13. Your rights and complaints

Depending on the circumstances, UK data-protection law may provide rights of access, rectification, erasure, restriction, portability, objection and safeguards relating to automated decisions. Where the request concerns Customer Content controlled by an organisation, ADEPTABLE may direct or forward the request to that organisation and assist it as processor.

Data-protection complaints can be sent to privacy@boardcue.live. ADEPTABLE will handle complaints in accordance with applicable statutory requirements. Individuals may also complain to the Information Commissioner's Office.

14. Changes and contact

We may update this policy as BoardCue, suppliers or applicable law change. We will publish the current version with its effective date.

Privacy: privacy@boardcue.live | General support: support@boardcue.live

Meeting Effectiveness

Where an organisation enables Meeting Effectiveness, eligible participants may provide seven ratings and optional comments during the seven days after a completed meeting. The customer organisation determines the purpose, lawful basis, eligible participants, access and retention rule for this processing.

In anonymous mode, organisation reporting does not identify respondents and suppresses aggregate scores and comments until at least three responses exist. BoardCue does not infer or surface individual effectiveness scores. Protected participant identifiers are retained to enforce eligibility, one response per participant and the response window.