

BoardCue Live Data Processing Agreement

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 DPA forms part of the agreement between ADEPTABLE LTD ("Processor") and the organisation purchasing or using BoardCue Live ("Customer" or "Controller") where ADEPTABLE processes personal data on the Customer's behalf.

1. Scope and instructions

This DPA applies only where ADEPTABLE acts as processor or subprocessor. ADEPTABLE will process Customer Personal Data only on the Customer's documented instructions, including instructions embodied in the Customer's use and configuration of BoardCue, except where law requires other processing.

2. Nature of the service and intended data scope

BoardCue provides governance intelligence, board/committee content management, meeting support, search, AI analysis and governance workflows.

BoardCue is not intended to replace sector-specific operational systems or to act as the primary repository for routine individual case-management records or datasets. The Customer may nevertheless lawfully include personal or special-category information where it is necessary for a governance purpose, in which case that information is Customer Personal Data under this DPA.

3. Confidentiality and security

ADEPTABLE will ensure that personnel authorised to process Customer Personal Data are subject to appropriate confidentiality obligations and access data only where necessary.

ADEPTABLE will implement and maintain technical and organisational measures appropriate to risk, taking into account the state of the art, cost, and the nature, scope, context and purposes of processing. The current framework is summarised in Schedule 2 and the Security and Information Governance Overview.

4. Customer responsibilities

- determine and document the applicable Article 6 basis and any Article 9, criminal-offence or sector-specific condition;
- meet transparency obligations, including to meeting participants;
- decide whether transcription is lawful and proportionate and approve the browsers/devices its users may use;
- configure roles, committee access and MFA appropriately;
- apply data minimisation and retention requirements;
- respond to data-subject requests as controller and complete a DPIA where required; and
- ensure BoardCue is not used as the sole basis for unlawful solely automated or other high-impact decisions.

5. Subprocessors

The Customer gives general written authorisation for ADEPTABLE to appoint subprocessors needed to provide BoardCue. ADEPTABLE will maintain a current Subprocessor Register, conduct proportionate due diligence, impose applicable written data-protection obligations, and remain responsible for subprocessor performance to the extent required by law.

ADEPTABLE will provide advance notice of a material new subprocessor where reasonably practicable, with a target of at least 15 days before routine processing of existing Customer Personal Data. Emergency changes required for security, law or service continuity may occur on shorter notice.

6. International transfers

ADEPTABLE will not knowingly make a restricted transfer of Customer Personal Data for which it is responsible unless a lawful transfer route is in place. The authoritative Subprocessor Register identifies verified destination and transfer information and flags vendor-confirmation points.

7. Data-subject rights and DPIAs

Taking into account the nature of processing, ADEPTABLE will provide reasonable assistance to enable the Customer to respond to valid data-subject requests and to carry out DPIAs or regulator consultation where required.

8. Personal data breaches

ADEPTABLE will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data for which ADEPTABLE acts as processor.

Where practicable, ADEPTABLE's operational target is to provide an initial customer notice within 24 hours of becoming aware of the personal data breach. ADEPTABLE will not delay the initial notice solely because the investigation is incomplete or all facts have not yet been confirmed.

Information may be provided in phases. To the extent known, the notice will describe the nature of the breach, awareness time, affected service/data, approximate categories and numbers of affected data subjects/records, likely consequences, containment/mitigation, contact point and information reasonably required for the Customer's own notification assessment.

9. Audits and information rights

ADEPTABLE will make available information reasonably necessary to demonstrate compliance with Article 28 and this DPA. A Customer may conduct a reasonable audit no more than once in any 12-month period unless a regulator requires more or a relevant material incident justifies it. The parties will normally use a staged evidence-first approach.

10. Return, export and deletion

At the end of the services, at the Customer's choice, ADEPTABLE will delete or return Customer Personal Data and delete existing copies unless UK law requires storage.

Where the Full Organisation Exit workflow is included in the order form and enabled for the deployment, the organisation workspace becomes read-only at termination, ADEPTABLE makes a full organisation export available to authorised organisation administrators for 14 calendar days after notification that it is ready, and active-system deletion begins when that window ends unless the Customer requests immediate deletion or gives another lawful instruction.

ADEPTABLE's target is to complete active-system deletion within 30 days after the applicable export window or deletion instruction. Protected backups are put beyond normal use and expire through the ordinary verified backup lifecycle. If a backup is restored, the deletion state must be reapplied before data returns to ordinary use.

11. Term and liability

This DPA continues while ADEPTABLE processes Customer Personal Data on the Customer's behalf. Liability is subject to the main agreement unless law or an order form provides otherwise.

Schedule 1: Processing details

Subject matter

Description: Provision of BoardCue Live as a governance intelligence, meeting and governance-operations platform.

Duration

Description: Customer agreement plus agreed return/deletion period and protected backup lifecycle.

Purpose

Description: Hosting/search of governance material; AI analysis; transcription; meeting preparation/follow-through; actions, decisions, approvals and workflows; notifications; security/audit; authorised support.

Personal data

Description: Names, roles and professional contact details; meeting attendance/contributions; transcripts; opinions, decisions, actions and accountability information; workforce information; incident/complaint/safeguarding information where lawfully included; authentication/access/audit metadata; other personal data lawfully placed in Customer Content.

Sensitive data

Description: Special-category or criminal-offence information may occur where necessary for governance, but patient-level clinical datasets are outside intended use.

Data subjects

Description: Board/committee members, executives, employees/workers, meeting participants, complainants, whistleblowers, advisers and other people referred to in governance material. Patients/service users or other members of the public may be referred to incidentally in governance material, but are not intended as a routine BoardCue dataset.

Schedule 2: Technical and organisational measures

- authenticated user access and Supabase-backed identity controls;
- organisation administrators can require MFA for organisation users;
- role and committee access restrictions and row-level database controls;
- audit logging for relevant governance/security events;
- rate and payload limits on sensitive routes;
- controlled support access with explicit authorisation, time limits, revocation and read-only default;
- TLS/HTTPS in production deployment;

- quarantine and fail-closed attachment handling where malware scanning is configured;
- governance export capabilities and deletion-integrity controls as implemented;
- production Supabase primary database and document-storage region: United Kingdom; enterprise go-live requires Pro or higher under the current assurance baseline.

Schedule 3: Authorised subprocessors

The authoritative list is the BoardCue Subprocessor and Data Flow Register. Cloud AI processing uses direct Google Gemini Developer API and OpenAI API accounts controlled by ADEPTABLE. Browser/OS speech-recognition providers selected through the customer's endpoint environment are not automatically ADEPTABLE subprocessors.