

Data Processing Addendum

Cognivio Ltd. (in formation) — Version 2.1 — Forms part of the Agreement with the Customer

1. Definitions

Capitalised terms not defined here have the meaning in the Agreement or the Cognivio Privacy Policy. "Data Protection Laws" means all laws applicable to the processing of Personal Data under this DPA, including Israel's Protection of Privacy Law 5741-1981 and the Privacy Protection (Data Security) Regulations 5777-2017; the EU GDPR; the UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025; and, in the United States, FERPA, COPPA and applicable state student-privacy and biometric-privacy laws. "Customer Data" means Student Data and Teacher Data processed by Cognivio on behalf of Customer. "Sub-processor List" means the list published at <https://cognivio.live/legal/subprocessors>, as updated in accordance with Section 7.

2. Roles

2.1 Customer is the controller (or database owner, educational agency or equivalent) of Customer Data and determines the purposes and lawful basis for recording and processing.

2.2 Cognivio is the processor (or holder / school official / service provider, as applicable) of Customer Data and processes it only on Customer's documented instructions, which consist of the Agreement, this DPA, the Service's functionality as configured by Customer, and any further written instruction.

2.3 Cognivio is an independent controller of account-administration, security-log and billing data, and independently determines the use of Non-Identifiable Data as set out in Section 9.

2.4 Cognivio will inform Customer if an instruction in its opinion infringes Data Protection Laws, and may suspend the instruction until resolved.

3. Scope of processing

Item	Description
Subject matter	Classroom video and audio, transcripts, AI analysis of instructional practice, coaching content, account and usage data
Duration	Term of the Agreement plus the deletion period in Section 11
Nature and purpose	Hosting, privacy rendering (blurring), storage, AI analysis, presentation to authorised users, deletion — solely to provide the Service
Data subjects	Teachers and other educators; school personnel; students appearing incidentally in recordings
Categories	Identity and contact data; authentication data; teacher enrollment photographs; classroom image, audio and speech; instructional-practice analysis; coaching content; technical and audit data
Special categories	Transient facial-recognition computation against the consenting teacher's reference photographs (no template or embedding stored); classroom recordings may incidentally reveal other special-category data, which the Service does not extract or infer

4. Customer obligations

Customer is responsible for: determining the lawfulness of recording in its jurisdiction; providing all notices and obtaining all consents required for recording and processing (including parental consent and biometric-law consent where applicable); its users' compliance with the Agreement; its access and role decisions within the Service; and providing documented instructions. Customer acknowledges that Cognivio does not monitor classrooms and cannot verify that consents have been obtained.

5. Cognivio obligations

Cognivio will: (a) process Customer Data only on Customer's instructions; (b) implement the technical and organisational measures in Annex A and not reduce them during the Term; (c) apply the privacy-pipeline invariants in the Privacy Policy (blur by default per frame, add-only blur, fail-closed, automated release gate, destruction of raw uploads) as non-configurable features of the Service; (d) ensure persons authorised to process Customer Data are bound by confidentiality; (e) assist Customer with data-subject requests, data-protection impact assessments and regulator consultations to the extent reasonably required; (f) maintain records of processing; (g) not sell Customer Data, use it for advertising, or use it to build profiles of students; and (h) not use Customer Data to train or improve any model except as permitted for Non-Identifiable Data in Section 9.

6. Personnel and access

Access to unblurred material and to production systems is restricted to named Cognivio personnel whose role requires it and is logged. Cognivio will require any such person to complete background verification to the extent permitted by law, privacy and security training, and written confidentiality undertakings before access is granted, and will maintain a current list of such persons available to Customer on request.

7. Sub-processors

7.1 Customer authorises the sub-processors on the Sub-processor List as at the Effective Date, currently: MongoDB Inc. (Atlas database, AWS il-central-1), Cloudflare Inc. (R2 object storage, EU jurisdiction), Railway Corp. (application hosting, US), Google LLC (Gemini AI, US), Anthropic PBC (Claude AI, US) and Resend Inc. (transactional email, US).

7.2 Cognivio will give Customer at least 30 days' notice before engaging a new sub-processor that will process Customer Data. Customer may object on reasonable data-protection grounds; if the objection cannot be resolved, Customer may terminate the affected Service without penalty.

7.3 Cognivio will impose on each sub-processor written obligations no less protective than this DPA, including no use of Customer Data for the sub-processor's own purposes, no model training on Customer Data, and security commitments, and remains liable for its sub-processors' performance.

7.4 Cognivio will configure each AI sub-processor so that Customer Data is not retained beyond the period stated in the Sub-processor List, and will pursue zero-data-retention configuration where offered.

8. Security incidents

Cognivio will notify Customer without undue delay after becoming aware of a Personal Data breach affecting Customer Data, and in any event within 48 hours (or any shorter period required by law applicable to Customer, including the Israeli Ministry of Education supplier standard where Customer is regulated by it), with the information reasonably required for Customer to meet its own notification obligations, and will cooperate in investigation and remediation. Where the incident originates with a sub-processor, Cognivio will pass through any credits, remedies or indemnities received to the extent permitted by its agreements with that sub-processor.

9. Non-Identifiable Data

9.1 Cognivio may create Non-Identifiable Data from Customer Data in accordance with its De-identification Standard (Annex B) and use it to operate, maintain, improve and develop the Service, including to train, validate and refine analytical and machine-learning models and to develop related professional-learning features.

9.2 Cognivio will not attempt to re-identify Non-Identifiable Data, will not use it for advertising or consumer profiling, and will contractually prohibit any recipient from re-identification. Non-Identifiable Data is not disclosed to third parties except to a successor under Section 12 or to service providers processing it on Cognivio's behalf under equivalent restrictions.

9.3 Where Customer is subject to a regulator or standard that requires specific approval for such use (including the Israeli Ministry of Education supplier standard §4.9.9), Cognivio will not create Non-Identifiable Data from that Customer's data until the approval has been obtained or Customer confirms in writing that it is not required.

10. Biometric processing

The Service stores no biometric template or embedding of any person. The enrolled teacher's reference photographs, provided with her written in-product consent, are used solely to leave her unblurred: the privacy pass computes a comparison transiently, in memory, and discards it. The photographs are stored encrypted at rest and deleted on the teacher's withdrawal of consent or account closure in accordance with the Retention Policy. Face detection applied to other persons in a recording likewise computes transient measurements only; no crop, embedding or template is persisted, and the processing record retains only face coordinates and match flags. Customer is responsible for determining whether biometric-law notices or consents are required in its jurisdiction and, where Customer operates in a jurisdiction with a biometric privacy statute, for ensuring teacher enrollment satisfies its requirements.

11. Return and deletion

11.1 During the Term, Customer and its authorised users may delete Customer Data through the Service; deletion removes the recording and all derived identifiable data.

11.2 On termination, or on Customer's written instruction at any time, Cognivio will within 30 days delete all Customer Data (other than Non-Identifiable Data and records Cognivio must retain by law, which will be retained only for that purpose) from production systems and, on request, provide an export in a standard format before deletion. Backups expire within the rotation period stated in the Retention Policy. Cognivio will confirm deletion in writing.

11.3 Org export contents and exclusions stated; the offboarding sequence in order (export on request → notify teachers to take their own → delete → confirm in writing).

12. Change of control

If Cognivio undergoes a merger, acquisition or sale of substantially all its assets, Customer Data may be transferred to the successor only if the successor is bound by this DPA and the Privacy Policy in respect of that data. Cognivio will notify Customer before the transfer takes effect and Customer may instruct deletion of its Customer Data before transfer.

13. Audits and information

Cognivio will provide Customer with information reasonably necessary to demonstrate compliance with this DPA, including its Information Security Program, sub-processor certifications and, once available, penetration-test summaries and ISO 27001 status, and will complete Customer's reasonable security questionnaires within 14 days. Customer may conduct an audit, itself or through an independent auditor bound by confidentiality, on 30 days' written notice, no more than once per year unless required by a regulator or following an incident, and remotely unless an on-site audit is required by Data Protection Laws applicable to Customer.

14. International transfers

Transfers of Customer Data from the EU to Israel rely on the European Commission's adequacy decision for Israel. Transfers of Customer Data from the United Kingdom to Israel and to the European Economic Area rely on the United Kingdom's adequacy regulations, and any other transfer of personal data subject to UK data-protection law is made as set out in Annex C-1. Transfers to sub-processors outside Israel and the EU rely on the transfer mechanism identified in the Sub-processor List for that sub-processor. Where Customer is regulated by the Israeli Ministry of Education, Cognivio will process and store Customer Data in Israel in accordance with the Ministry's supplier standard from the date the Israel deployment is certified to Customer, and until that date will disclose in writing each processing step that occurs outside Israel.

15. US-specific terms

Where Customer is a US educational agency or institution: Cognivio is a "school official" with a legitimate educational interest under FERPA, under Customer's direct control with respect to use and maintenance of education records, and will not re-disclose personally identifiable information from education records except as instructed; Cognivio will comply with COPPA in reliance on Customer's authorisation on behalf of parents for the school's educational purpose; and Cognivio will comply with applicable state student-privacy laws, including not selling student information, not targeting advertising, and not building student profiles for non-educational purposes. Customer's state-specific requirements (for example New York Education Law 2-d parents' bill of rights) are set out in Annex C where applicable.

16. General

This DPA is governed by the law governing the Agreement, without prejudice to mandatory Data Protection Laws applicable to Customer. In case of conflict on data-processing matters, this DPA prevails. Where a jurisdiction-specific term in Annex C applies to Customer, that term prevails over the body of this DPA for the data it covers. Liability is as set out in the Agreement.

Annex A — Technical and organisational measures (summary)

Area	Measure
Privacy pipeline	Blur-by-default per frame; add-only blur; automated quality checks as the release gate; staff view recordings only to troubleshoot; fail-closed quarantine; raw upload destroyed on verification
Data separation	The Wall: teacher-private data unreachable by any Customer role, enforced at query, payload and computation layers; organisation analytics computed server-side
Tenancy and access	Organisation-sovereign tenants; role-based access; least-privilege service access via a storage gateway; no cross-tenant paths
Encryption	TLS in transit; AES-256 at rest for database and backups; object storage encrypted

Area	Measure
	at rest (AES-256)
Authentication	Hashed passwords (bcrypt); JWT sessions; in-app multi-factor authentication available to administrators and teachers (enabled in account settings); SSO on the roadmap
Logging	Durable audit collections for privacy events, deletions and admin alerts; pipeline job records; platform logs
Deletion	Zero-residue per-video deletion across all collections, verified in production; deletion audit trail
Containment	Kill-switch flags for privacy wall, coaching layer and AI budget; quarantine states
Personnel	Named access only; confidentiality; logged production access

Annex B — De-identification Standard (summary)

Non-Identifiable Data must: contain no direct identifiers; carry no lesson, school, teacher, student, tenant or upload identifiers and no key linkable to them; contain no imagery, facial templates, voiceprints or other biometric data; contain no verbatim classroom speech attributable to a student and no verbatim teacher speech longer than a short phrase; be derived by abstraction (event sequences, timing, counts, skeletal or motion abstractions) or aggregation; be released into any development dataset only when the contributing pool meets the minimum-group threshold set in the Standard; and be documented with the transformation applied. The full Standard is maintained in Cognivio's Privacy Operations Procedures.

Annex C — Jurisdiction-specific terms

C-1 United Kingdom. Where UK data-protection law applies to Customer Data, the Cognivio UK Data Protection Addendum (version 1.0) applies as Annex C-1 to this DPA. It takes effect when accepted by a person authorised to bind Customer, as set out in it.

Further jurisdiction-specific terms agreed with a Customer are added as further annexes (C-2 onwards).