

Cognivio Privacy Policy

Cognivio Ltd. (in formation) — Version 2.1 — Effective date: October 5, 2026

1. Who we are and what this Policy covers

Cognivio Ltd. ("Cognivio", "we") provides a teacher observation and coaching platform (the "Service"). Teachers record and upload classroom lessons; the Service produces a private coaching experience for the teacher and rubric-aligned professional-growth views for the teacher's school.

This Policy applies to the Service, to app.cognivio.live and cognivio.live, and to all data processed through them. It should be read together with our Data Processing Addendum (DPA), Data Retention Policy and Sub-processor List, which form part of our commitments to schools.

The Service is designed to support schools in meeting their own obligations. Schools remain responsible for their use of the Service and for the lawfulness of classroom recording in their jurisdiction.

2. Our role

School as controller. The school (or district, network, teacher-training institution or other educational organisation — the "Customer") decides whether lessons are recorded, for what purpose, and who may access them. For Student Data and Teacher Data the Customer is the data controller (or the equivalent under local law, such as the "database owner" under Israel's Protection of Privacy Law and the "educational agency" under FERPA and state student-privacy laws).

Cognivio as processor. We process Student Data and Teacher Data only to provide the Service, on the Customer's documented instructions and under the DPA. We decide technical means (hosting, security, analysis tooling) but not educational purposes.

Cognivio as independent controller for a narrow set of data: account administration, security logs, billing, and communications with the Customer.

Legal basis for our own processing. Where EU or UK data-protection law applies, we process account administration, security-log, billing and Customer-communications data on the basis of our legitimate interests in operating and securing the Service and administering our contract with the Customer, and where needed to comply with a legal obligation. We create Non-Identifiable Data (Section 8) on the basis of our legitimate interests in improving the Service, under the safeguards described there. For Student Data and Teacher Data, the Customer determines the legal basis.

Non-Identifiable Data. We independently determine how Non-Identifiable Data (Section 8) is used. Non-Identifiable Data is not personal data, and our use of it does not change our role as processor for Student Data or Teacher Data.

3. Definitions

- **Teacher Data:** personal data about a teacher or other educator using the Service, including account data, reference enrollment photos, recordings in which the teacher appears, transcripts, analysis outputs, coaching content and private reflections.
- **Student Data:** personal data relating to an identifiable student. In the Service this exists only incidentally — as a student's image or voice in a classroom recording or transcript. The Service creates no student accounts, profiles, identifiers, scores or analytics.

- **Teacher-Private Data:** the subset of Teacher Data that is never available to the Customer: private reflections, the teacher's coaching (Mira) conversations, self-view analytics and detailed feedback text. Enforced structurally (the "Wall", Section 6).
- **Organisation-Visible Data:** rubric-aligned professional-growth views derived from the AI analysis, expressed as trends and descriptions across areas of practice, made available to Customer roles under the Customer's access rules.
- **Non-Identifiable Data:** data derived from the Service that has been de-identified, aggregated or abstracted in accordance with our De-identification Standard so that it cannot reasonably be linked to any school, teacher, student or lesson.

4. Data we process

4.1 Account and administrative data

Name, email, role, organisation, authentication credentials (passwords are stored hashed), invitation and support communications, billing contacts.

4.2 Teacher enrollment and consent data

Reference photographs of the teacher captured during enrollment (multi-pose) and the teacher's recorded consent status. No facial template or embedding is stored: matching against the photographs is computed transiently during the privacy pass and discarded. The photographs are used for one purpose only: to recognise the consenting teacher so that she is not blurred. They are never used to identify anyone else.

4.3 Classroom recordings and derived content

Video and audio of lessons; the blurred ("rendered") version produced by our privacy pipeline; face-detection results retained on the processing record (coordinates and match flags only, no imagery); transcripts where transcription is enabled (it is disabled as of the effective date, and talk-time attribution is produced at class level only); the AI analysis of instructional practice; teacher feedback and coaching content; and the trends derived for Organisation-Visible views.

4.4 Technical and usage data

Device and browser information, IP address, timestamps, application and security logs, pipeline job records, and audit records of privacy-relevant actions (uploads, reviews, deletions, access to quarantined material). We do not use analytics, telemetry or session-recording tools in the Service or on our website.

5. How recordings are protected: the privacy pipeline

The following are engineered invariants of the Service, verified in production, not configurable options:

1. **Every face is blurred by default, in every frame.** Only faces that match the enrolled, consenting teacher are left visible. Faces that cannot be matched, or where confidence is insufficient, are blurred.
2. **Detection can only add blur.** No component of the pipeline can remove blur that another component applied.
3. **Fail-closed.** If the pipeline cannot complete the privacy pass, or the automated quality check is not satisfied, the recording is quarantined and never released.
4. **Automated release gate.** Automated quality checks screen every rendered recording before release. Cognivio staff do not routinely view recordings; they view one only where needed to troubleshoot a specific problem.

5. **The original is destroyed.** The raw, unblurred upload is deleted promptly after the rendered version is verified, by an automated process. We do not retain unblurred source video of released recordings. While a recording is held, the original is kept only until release or until the 30-day hold period in the Data Retention Policy expires.
6. **Blur cannot be switched off by a user.** The Customer may authorise unblurred rendering for a specific class only under a written Unblurred Recording Authorisation, after confirming that all legally required consents are on file. Teachers cannot opt out of blurring on their own. See Section 9.

6. The Wall: what the school does not see

Teacher-Private Data is structurally unreachable from any Customer-facing role. This is not a permission setting; it is enforced at the query, payload and calculation layers of the Service, and organisation-facing analytics are computed on the server so that underlying per-teacher numbers never leave it. Customer roles see Organisation-Visible Data only, as trends and descriptions built on the Customer's own rubric.

Lessons a teacher chooses to share. The one exception is a lesson the teacher chooses to share. A teacher may share a specific lesson, including its blurred recording, its feedback and how the lesson followed the teacher's lesson plan (with short quotes from the plan), with colleagues or school roles at the Customer. Sharing is always the teacher's own action, and a Customer role cannot open a lesson the teacher has not shared. A teacher can stop sharing at any time, and access ends immediately.

7. AI processing

7.1 What the AI does

One AI analysis is produced per lesson, focused on instructional practice (for example questioning, pacing, wait time, talk patterns, feedback moves). That single analysis is then presented in two role-specific forms. The AI is descriptive: it reports what occurred and invites reflection. Detailed per-area scores are shown only to the teacher whose lesson it is. The AI does not rank teachers, does not make or recommend employment decisions, and does not produce any output about an individual student.

7.2 What the AI does not do

The Service does not perform emotion recognition, does not infer sensitive characteristics of any person, does not categorise anyone by biometric traits, does not identify students, and does not create or retain any biometric template of anyone. During the privacy pass, transient measurements are computed in memory for every detected face solely to test whether it is the consenting teacher; nothing is persisted.

7.3 Mira

Mira is an AI coaching assistant available to teachers. Teachers are informed that they are interacting with an AI. Mira operates on a propose-confirm-execute basis for any action it takes on the teacher's behalf, and its conversations are Teacher-Private Data.

7.4 AI providers

AI analysis runs on models provided by Google (Gemini) and Anthropic (Claude), listed in our Sub-processor List. Neither provider uses our data to train its models. As of the effective date, the analysis and detection steps send the original recording to Google and the quality check sends frames of the blurred recording; we are moving analysis to the blurred recording and detection to a contractual zero-retention configuration. Provider-side retention (for example short-term file storage and abuse-monitoring logs) is described in the Sub-processor List, which records the current status for each provider.

7.5 Model improvement

We do not train, fine-tune or evaluate our models on identifiable Teacher Data or Student Data. See Section 8.

8. Non-Identifiable Data and product improvement

We create and use Non-Identifiable Data to operate, maintain, improve and develop the Service, including to train, validate and refine our analytical and machine-learning models, to develop new professional-learning features, and for internal research and benchmarking.

Non-Identifiable Data is produced under a written De-identification Standard that requires, at minimum: removal of all direct identifiers; no lesson, school, teacher or student identifiers or linkable keys; no facial imagery, facial templates, voiceprints or other biometric data; no verbatim classroom speech attributable to a student; aggregation or abstraction (for example interaction sequences, timing patterns, and skeletal or motion abstractions rather than imagery); and minimum-group thresholds before release into any development dataset.

We will not attempt to re-identify Non-Identifiable Data and we contractually prohibit anyone who receives it from doing so. We do not use Non-Identifiable Data for advertising, behavioural profiling or any product directed at consumers.

Where a jurisdiction or a Customer's regulator (for example the Israeli Ministry of Education's supplier standard) requires specific approval for derivative use of data, we obtain it before such use in respect of that Customer.

9. Unblurred recordings

Blurring is the default and cannot be disabled by an individual user. A Customer may request unblurred rendering for a defined class or programme where its own legal analysis supports it, by executing our Unblurred Recording Authorisation, which requires the Customer to confirm that all required notices and consents (including parental consent and, where applicable, biometric-law consent) are in place and to assume responsibility for that determination. Unblurred recordings are processed under heightened controls described in that Authorisation and in the Retention Policy. Cognivio may decline an Authorisation in any jurisdiction where it is not satisfied the arrangement is lawful.

Exemplary lessons ("Gold Star"). A teacher may designate a recording as exemplary for viewing by other authorised users only with the teacher's explicit action and the Customer's approval. Exemplary recordings are blurred; unblurred exemplary recordings require an Unblurred Recording Authorisation covering that use.

10. Sharing and disclosure

We disclose data only:

- to users the teacher or Customer has authorised, within the access rules of the Service;
- to our sub-processors, listed in the Sub-processor List, under written terms no less protective than our DPA;
- when required by law or valid legal process, after notifying the Customer where legally permitted; and
- to a successor in a merger, acquisition or other change of control, provided the successor is bound by this Policy and the DPA for all data transferred, and Customers are notified in advance with the right to delete their data before transfer.

We do not sell personal data, do not share it for advertising, and do not disclose it to any third party for that third party's own purposes.

11. Sub-processors and infrastructure

Our current sub-processors, what each does, where it processes data and its data-protection status are set out in the Sub-processor List, which we keep current and which we will notify Customers of before adding a new sub-processor that will process Student Data or Teacher Data. As of the effective date the list comprises MongoDB Atlas (database, AWS Israel region), Cloudflare R2 (video storage, EU jurisdiction), Railway (application hosting, United States), Google (Gemini AI, United States), Anthropic (Claude AI, United States) and Resend (transactional email, United States).

12. International transfers

Cognivio is established in Israel. Where personal data is transferred across borders we rely on Israel's EU adequacy decision, on the Customer's authorised transfer mechanism where the Customer is outside the EU/Israel, and on contractual and technical safeguards with sub-processors (encryption in transit and at rest, access controls, no-training and retention commitments). For personal data subject to UK data-protection law, transfers to Israel and to the European Economic Area rely on the United Kingdom's adequacy regulations, and other transfers rely on the UK Extension to the EU-US Data Privacy Framework, the Information Commissioner's International Data Transfer Addendum or International Data Transfer Agreement, as set out in our UK Data Protection Addendum. Israeli Ministry of Education-regulated Customers are provisioned on our Israel deployment in accordance with the Ministry's residency requirements once that deployment is complete; until then such Customers are told precisely which processing occurs outside Israel and may decline to proceed.

13. Security

We maintain technical and organisational measures appropriate to the sensitivity of classroom recordings, including encryption in transit (TLS) and at rest, role-based access within organisation-sovereign tenants, least-privilege service access, audit logging of privacy-relevant actions, multi-factor authentication available to administrators and teachers, secrets management, and the fail-closed privacy pipeline described in Section 5. Our Information Security Program, which describes these measures in full and is updated as controls are added, is available to Customers on request.

Personnel. Access to unblurred material and to production systems is limited to named Cognivio personnel whose role requires it, is logged, and is subject to confidentiality obligations. As of the effective date that is a single founder-operator. Any additional personnel granted such access will first complete background verification to the extent permitted by law, privacy training and written confidentiality undertakings.

14. Retention and deletion

We keep personal data only as long as needed for the purpose for which it was collected, and then delete it. Our Data Retention Policy sets out the period for each category. In summary:

- Raw uploads: deleted on verification of the rendered version.
- Rendered recordings (and transcripts, where enabled): deleted at the end of the school year in which they were made (after a 60-day notice period) unless the teacher and the Customer both elect to retain a specific recording.
- Teacher analysis and coaching content: retained for the teacher's use while her account is active; deletable by the teacher at any time; deleted on account closure.
- Non-Identifiable Data: retained as it is not personal data.
- Account, security and audit data: retained for the periods in the Retention Policy.

Teachers can delete any recording in-product, and deletion removes the recording and everything derived from it. Customers may instruct deletion of any data at any time and receive written confirmation. Deleted data leaves backups within the backup rotation period stated in the Retention Policy.

15. Rights of individuals

Teachers can see in-product everything the Service holds about them. Depending on applicable law, teachers, students and parents may have rights of access, correction, deletion, restriction, portability and objection. Because the Customer is the controller, requests about Student Data should be made to the school, and we will assist the school in responding within the time limits that apply by law. If we receive a request about Student Data directly, we pass it to the school within 5 working days. Teachers may contact us directly for Teacher Data. Parents may inspect and seek correction of education records through their school in accordance with FERPA and equivalent laws. In the United Kingdom, anyone may also complain to the Information Commissioner's Office (ico.org.uk). We would welcome the chance to address a concern first.

16. Children

The Service is for use by educators and is not directed at children. Students do not have accounts and we do not knowingly collect personal information directly from children online. Student Data that appears incidentally in recordings is processed only on the school's instruction, only for the school's educational purpose, is minimised by blurring, is never used for advertising or profiling, and is retained only as set out in the Retention Policy. Where COPPA applies, we rely on the school's authorisation given on behalf of parents for the school's educational purpose and we do not use Student Data for any other purpose.

17. Incidents

If we become aware of a security incident affecting personal data we will notify affected Customers without undue delay and within the timelines required by applicable law and contract (including the Israeli Ministry of Education's timelines for regulated Customers and GDPR's 72-hour controller notification), provide the information Customers need to meet their own obligations, and cooperate in remediation.

18. Changes

We will not materially reduce the protections in this Policy for Student Data or Teacher-Private Data without prior notice to Customers. The current version and a change log are available at <https://cognivio.live/legal>.

19. Governing law and contact

This Policy is governed by the laws of the State of Israel, without prejudice to mandatory data-protection, education or consumer laws that apply based on the Customer's location.

Privacy contact: privacy@cognivio.live. Privacy Protection Officer / Data Protection Officer: not currently appointed; privacy@cognivio.live handles all privacy matters. EU representative under GDPR Article 27: Cognivio does not currently serve Customers in the European Union and will appoint a representative before it does. UK representative under UK GDPR Article 27: Cognivio has not appointed a UK representative.