TrAIning-360

Data Processing Agreement

HCAIS PTE. LTD. · Version 1.1 — 24 November 2026 · privacy@training-360.com

This Data Processing Agreement (« **DPA** ») forms part of the agreement for the Training-360 service (the « **Agreement** ») between:

- **the Customer** named in the Agreement (the « **Controller** »); and
- **HCAIS PTE. LTD.**, a private company limited by shares incorporated in Singapore (UEN 202548381G), 160 Robinson Road, #14-04, Singapore Business Federation Centre, Singapore 068914, owner and operator of Training-360 (the « **Processor** »).

The Processor's representative in the European Union (Article 27 GDPR) is Cédric Galichon, Paris, France, privacy@training-360.com.

1. Definitions

Terms such as *personal data*, *processing*, *controller*, *processor*, *data subject*, *personal data breach* and *supervisory authority* have the meaning given in Regulation (EU) 2016/679 (« **GDPR** »). « **Customer Personal Data** » means the personal data the Processor processes on behalf of the Controller to provide the service. « **Subprocessor** » means any processor engaged by the Processor to process Customer Personal Data. « **SCCs** » means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914.

2. Roles and scope

2.1 The Controller determines the purposes and means of the processing of Customer Personal Data; the Processor processes it only on the Controller's behalf. Annex I describes the processing.

2.2 For its own purposes — managing the commercial relationship, billing, the security of the service, and its website — the Processor acts as an independent controller under its privacy notice; this DPA does not cover that processing.

3. Processor obligations

3.1 **Instructions.** The Processor processes Customer Personal Data only on the Controller's documented instructions — the Agreement, this DPA and the Controller's use and configuration of the service — including for transfers, unless required by law, in which case it informs the Controller first unless the law forbids it. It informs the Controller at once if it believes an instruction infringes data protection law.

3.2 **Confidentiality.** Everyone authorised to process Customer Personal Data is bound by confidentiality.

3.3 **Security.** The Processor implements the technical and organisational measures in Annex II and keeps them at least at that level for the term of the Agreement.

3.4 **Data subject requests.** The Processor assists the Controller, by appropriate measures and as far as possible, in answering requests from data subjects: the service lets the Controller export and erase a person's data, and the Processor forwards to the Controller without undue delay any request it receives directly.

3.5 **Assistance.** The Processor assists the Controller with its obligations under Articles 32 to 36 GDPR (security, breach notification, impact assessments, prior consultation), taking into account the nature of the

processing and the information available to it.

3.6 **Personal data breach.** The Processor notifies the Controller of a personal data breach affecting Customer Personal Data without undue delay and no later than **48 hours** after confirming it, with what is known of its nature, the data and people concerned, its likely consequences and the measures taken or proposed; it completes the information as it becomes available.

3.7 **Records.** The Processor keeps a record of its processing activities carried out on behalf of controllers (Article 30(2) GDPR).

4. Subprocessors

4.1 The Controller gives a general authorisation to the Subprocessors listed in Annex III.

4.2 The Processor informs the Controller of any intended addition or replacement of a Subprocessor at least **30 days** in advance, by e-mail to the Controller's administrators. The Controller may object on reasonable data protection grounds within that period; the parties then discuss in good faith, and if no solution is found the Controller may terminate the affected part of the service without penalty.

4.3 The Processor imposes on each Subprocessor, by contract, data protection obligations providing at least the same level of protection as this DPA, and remains liable to the Controller for its Subprocessors' performance.

5. International transfers

5.1 Customer Personal Data is hosted in the European Union (Paris, France). The Processor is established in Singapore, which has no adequacy decision; to the extent the Processor's processing involves a transfer of Customer Personal Data out of the EEA, the **SCCs, Module Two (controller to processor)**, are incorporated into this DPA by reference, with the Controller as data exporter and the Processor as data importer, and with these choices: Clause 7 (docking) applies; Clause 9(a) Option 2 (general written authorisation, 30 days' notice); Clause 11(a) optional language not used; Clause 13: the supervisory authority competent for the Controller; Clause 17: the law of France; Clause 18: the courts of Paris, France. Annexes I to III of this DPA serve as the SCCs' Annexes I to III.

5.2 Where a Subprocessor processes Customer Personal Data outside the EEA, the transfer is covered by that Subprocessor's standard contractual clauses (Module Three, processor to processor) or another transfer mechanism recognised by the GDPR.

5.3 If the Controller is subject to the UK GDPR or Swiss data protection law, the parties will, on request, add the UK International Data Transfer Addendum or the Swiss adaptations to the SCCs.

6. Audits

6.1 The Processor makes available to the Controller the information needed to demonstrate compliance with this DPA: its security policies, a summary of its security assessments and of independent test results when available, and answers to the Controller's reasonable security questionnaire, under confidentiality.

6.2 Where that information is not sufficient, the Controller may, once a year and with 30 days' written notice, carry out or mandate an independent auditor bound by confidentiality to carry out an audit, at its own cost, during working hours and without access to other customers' data. An audit required by a supervisory authority or after a personal data breach is not limited to once a year.

7. Return and deletion

7.1 At the end of the Agreement the Controller may export its data from the service. On the Controller's written request the Processor deletes Customer Personal Data within **30 days**; failing a request it is deleted or anonymised according to the retention periods in Annex I. Copies in backups expire within **35 days** of deletion.

7.2 The Processor may keep Customer Personal Data only where law requires it, and then protects it and processes it only for that purpose.

8. General

8.1 Liability under this DPA is subject to the limitations of the Agreement, except where the law forbids it.

8.2 In case of conflict: the SCCs prevail over this DPA, and this DPA prevails over the Agreement for the processing of Customer Personal Data.

8.3 This DPA lasts as long as the Processor processes Customer Personal Data. It is governed by the law of **France**; the courts of **Paris** have jurisdiction, without prejudice to the SCCs.

For the Controller	For the Processor — HCAIS PTE. LTD.
Name:	Name:
Title:	Title: authorised signatory
Date and signature:	Date and signature:

Annex I — Description of the processing

Parties. Data exporter: the Controller (contact: its administrator named in the Agreement). Data importer: HCAIS PTE. LTD., contact privacy@training-360.com; EU representative Cédric Galichon, Paris.

Data subjects. The Controller's staff who use the Studio (administrators, managers, editors); the Controller's trainees (employees, contractors, candidates or visitors it invites) who play its trainings; people who may appear in photos, videos or on-site captures the Controller provides.

Categories of personal data.

- Identification and contact: name, work e-mail, role; identifier and name from the Controller's LMS or company sign-in.
- Training activity: assignments, plays (dates, progress, answers, score, time), feedback, comments, certificates (name, training, date, score, verification code).
- Account and security: sign-in records, session data, IP address and browser signals for security and abuse prevention.
- Content the Controller provides: briefs, documents, photos, videos and on-site captures, which may show people.

Special categories. None intended. The Controller should not put special categories of data in the content it provides.

Nature and purpose. Hosting, creating, delivering and tracking immersive trainings for the Controller: storing, organising, displaying, transmitting to the Controller's systems (LMS, webhook, API) when the Controller sets it up, generating training content (text, voice, images) from the Controller's material, support.

Frequency. Continuous for the duration of the Agreement.

Retention.

Data	Kept
Plays	90 days if only opened; 730 days once started
Assignments	Anonymised 24 months after the last activity
Certificates	End of the Agreement + 1 year
All the Controller's data	End of the Agreement + 3 years, unless deletion is requested earlier (section 7)
Sign-in and security logs	Up to 1 year (audit trail: 400 days)
Backups	34 days

Subprocessors. See Annex III.

Annex II — Technical and organisational measures

Summary of the Processor's security policies (version 1.0, approved 2026-11-24), available in full under NDA.

Area	Measures
Governance	Written security policies approved by management and reviewed yearly; risk register reviewed quarterly; named security owner
Hosting	Amazon Web Services, Paris region, in a dedicated production account under organisation guardrails (no root use, two regions only, security services locked)
Encryption	TLS 1.2+ in transit with HSTS; encryption at rest of databases, files, backups and secrets; keys in AWS KMS / Secrets Manager, one key per use, rotated
Access — customers	Passwordless sign-in by single-use code or link (15 minutes); company single sign-on; roles with least privilege; server-side isolation between companies on every request; session revocation on deactivation
Access — staff	Least privilege; MFA on cloud and mail accounts; « view as customer » logged; quarterly access review; leavers removed the same day
Development	Every change through a pull request and an automated gate (type checks, thousands of tests including security tests); infrastructure as code; no production data in development
Vulnerabilities	Continuous dependency scanning; external vulnerability scans; internal security assessments; fixes within 7 days (critical), 30 (high), 90 (medium)
Monitoring	Threat detection (GuardDuty), access analysis, an audit trail protected from deletion, alarms on sensitive changes; audit logs kept 1 year
Availability	Daily backups kept 34 days in a vault locked against deletion; point-in-time recovery; deletion protection; restore procedure written and rehearsed
Incidents	Written incident response plan with severities; customer notice within 48 hours of a confirmed breach; yearly exercise
Suppliers	Checked before engagement and yearly; data processing terms with each
Data minimisation	Only the data the service needs; private trainings served through short-lived signed links; retention periods enforced automatically
Endpoints	Full-disk encryption and Microsoft Defender (antivirus, endpoint detection) on every staff laptop; screen lock required; central device management with Microsoft Intune (compliance checks, remote

Area	Measures
	lock and wipe) being rolled out in December 2026

Annex III — Subprocessors

Subprocessor	Service	Location of processing	Data
Amazon Web Services EMEA SARL (and its affiliates)	Hosting, database, storage, e-mail, sign-in, AI text and vision (Amazon Bedrock, EU), speech (Amazon Polly)	EU (Paris); speech for French in the United States (narration text only)	All Customer Personal Data (hosting); narration text (speech)
Microsoft Ireland Operations Ltd (Azure AI Speech)	Speech for some languages (Vietnamese, Indonesian, Thai, Ukrainian)	EU (France Central)	Narration text only
OpenAI, L.L.C.	Generation and editing of training images	United States	Text prompts; assembled panoramas of the Controller's site; the Controller's photos only with its recorded consent
Cloudflare, Inc. (Turnstile)	Robot check when opening a training or a capture link	Global	IP address, browser signals
Apple, Google, Mozilla push services	Optional notifications to the Studio and the trainee space	Global	Push address, notification text
Microsoft Ireland Operations Ltd (Microsoft 365)	The Processor's mailbox, for support requests	Asia-Pacific (HCAIS tenant, Singapore)	What the Controller's users write to us