

Creatrix Data Processing Addendum

Version 1.0 · Effective 20 April 2026

This is version 1.0. It remains permanently available at this address. Later versions are published alongside it and listed in the version history below.

This Data Processing Addendum (“**DPA**”) applies when the Anubavam company named in a customer’s agreement (the “**Processor**”) processes personal data on behalf of that customer (the “**Controller**”) in providing Creatrix software and services. Creatrix includes Creatrix Campus, Creatrix Datahub, Creatrix Connect and Creatrix AI.

This DPA forms part of the customer’s master service agreement or other agreement for Creatrix (the “**Agreement**”), at the version stated in the Agreement. It takes effect without separate signature. A customer that needs a signed copy may sign this version as published, without changing it.

The Agreement may include a **Processing Details** schedule, which records what is specific to that customer: the categories of data, the hosting region, the authorised sub-processors and the contacts. The Processing Details prevail over this DPA on those points. In all other respects, this DPA prevails over the Agreement for the processing of personal data.

1. Definitions

- “**Data Protection Laws**” means all laws on the protection of personal data that apply to the processing under this DPA, including those listed in Annex 3.
- “**Personal Data**” means information relating to an identified or identifiable natural person that the Processor processes on behalf of the Controller under the Agreement.
- “**Sensitive Personal Data**” means Personal Data treated as sensitive or special under Data Protection Laws. Examples are health or disability information, religious belief, and information about criminal or disciplinary matters.
- “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, Personal Data.

- **“Sub-processor”** means a third party or Anubavam group company that the Processor engages to process Personal Data on the Controller’s behalf.
- **“Sub-processor List”** means the list published at <https://www.creatrixcampus.com/legal/subprocessors>, at the version stated in the Agreement.

Other capitalised terms have the meanings given in the Agreement.

2. Roles and instructions

2.1 The Controller determines the purposes and means of processing. The Processor processes Personal Data only on the Controller’s documented instructions. These include instructions given through the Agreement, the configuration of the Software, and submissions the Controller makes to regulators through the Software. The only exception is where law requires otherwise, in which case the Processor informs the Controller first unless the law forbids it.

2.2 The Controller warrants that it has a lawful basis for the processing, and that its instructions comply with Data Protection Laws.

2.3 The Processor shall tell the Controller if, in its opinion, an instruction infringes Data Protection Laws. It may suspend the affected processing until the instruction is confirmed, withdrawn or amended.

2.4 The Processor shall not sell Personal Data, or use it for its own purposes. This includes advertising and training artificial intelligence models made available to others.

3. Processor obligations

3.1 The Processor shall:

- (a) ensure that everyone authorised to process Personal Data is bound by confidentiality obligations and receives data protection training;
- (b) apply the technical and organisational measures in Annex 2;
- (c) assist the Controller, taking into account the nature of the processing, with security, breach notification, data protection impact assessments and consultation with regulators;
- (d) make available the information reasonably necessary to demonstrate compliance with this DPA; and
- (e) notify the Controller if it becomes aware that it can no longer meet its obligations under this DPA.

3.2 The Processor's privacy function can be reached at dpo@anubavam.com.

4. Security

4.1 The Processor maintains an information security management system certified to ISO/IEC 27001:2022 and a privacy information management system certified to ISO/IEC 27701:2019. Certificates are available on request.

4.2 Each customer's production environment is dedicated to that customer and isolated from other customers. Shared regional integration services, such as Creatrix Connect, are tenant-isolated and hold Personal Data only in transit.

4.3 The Processor may update the measures in Annex 2, provided the overall level of protection is not reduced.

5. Sub-processors

5.1 The Controller authorises the Processor to engage the Sub-processors on the Sub-processor List that apply to the Controller's services and hosting region. If the Processing Details name the authorised Sub-processors, only those are authorised.

5.2 The Processor shall give at least thirty (30) days' notice before adding or replacing a Sub-processor, by email to the Controller's privacy contact and by updating the Sub-processor List.

5.3 The Controller may object on reasonable data protection grounds within fourteen (14) days of the notice. The Parties shall discuss the objection in good faith. If it is not resolved and the Processor cannot provide the services without the new Sub-processor, either Party may terminate the affected services on thirty (30) days' notice. The Controller is then refunded the prepaid fees for the unused period.

5.4 The Processor shall impose on each Sub-processor data protection obligations at least as protective as this DPA. It remains liable for each Sub-processor's acts and omissions.

6. Location and transfers

6.1 Personal Data is hosted and processed in the Controller's contracted hosting region, as stated in the Agreement. This covers production data, backups and logs.

6.2 Personal Data is not stored outside the contracted hosting region without the Controller's prior written consent. The only exception is limited Personal Data appearing in individual support communications, through the support tools on the Sub-processor List. Data extracts are never exchanged this way.

6.3 Where a Sub-processor or Anubavam group company accesses Personal Data remotely from another country, for support, incident response or disaster recovery, that access:

- (a) is limited to named personnel, is logged, and is protected by multi-factor authentication;
- (b) does not involve downloading or storing Personal Data outside the hosting region; and
- (c) is subject to the safeguards required by Data Protection Laws for such access, including any contractual clauses Annex 3 requires.

6.4 The Controller may require, in its Processing Details, that support access to its environment takes place only from within its hosting country.

7. Artificial intelligence

7.1 Creatrix AI processing runs within the Controller's contracted hosting region, on in-region model services.

7.2 Personal Data, prompts and outputs are not used to train or improve any model made available to any other customer or third party.

7.3 Where an AI suggestion would change a record, a person approves the change unless the Controller configures otherwise.

8. Personal Data Breach

8.1 The Processor shall notify the Controller promptly on becoming aware of a Personal Data Breach, and in any event within forty-eight (48) hours. Initial notice is not delayed while details are gathered. Notification goes to the Controller's privacy contact and is sent from incidents@anubavam.com.

8.2 The notification shall describe, as far as is known at the time:

- the nature of the breach;
- the categories and approximate number of data subjects and records affected;
- the likely consequences; and
- the measures taken or proposed.

Further information is provided in phases as it becomes available.

8.3 The Processor shall cooperate with the Controller's investigation and remediation.

8.4 The Processor shall not notify a regulator or any data subject about a breach of the Controller's Personal Data without the Controller's consent, unless the law requires it to.

9. Data subject requests

9.1 The Software lets the Controller access, correct, export and delete Personal Data.

9.2 The Processor shall forward any request it receives from a data subject to the Controller within five (5) business days. It shall not respond to the request, other than to acknowledge it, and shall otherwise assist the Controller as reasonably required.

10. Retention, return and deletion

Data	Retention
Personal Data in the Software	The term of the Agreement. After expiry, available to the Controller for export for ninety (90) days
Audit and access logs	Up to twelve (12) months
Backups	Overwritten in the ordinary backup cycle (Annex 2)
Data in transit to a regulator or third-party system	Until the recipient responds, then purged. Only metadata and a hash are retained

10.1 At the end of the export period, or earlier on the Controller's written request, the Processor shall securely delete Personal Data from active systems within thirty (30) days and certify the deletion in writing. Backup copies expire in the ordinary backup cycle, up to twelve (12) months. Until then they remain protected under this DPA and are used only for disaster recovery. Any Personal Data restored from a backup is deleted again. If the Controller asks, the Processor shall first return the data in a commonly used machine-readable format.

10.2 Where law requires the Processor to retain any data, it shall tell the Controller what it retains and why, and shall keep that data protected under this DPA.

11. Audit

11.1 Once in any twelve (12) month period, the Processor shall provide on request:

- its current certifications;
- a summary of its most recent independent security assessment; and
- answers to a reasonable security questionnaire.

11.2 If that evidence does not reasonably demonstrate compliance, or after a material Personal Data Breach, credible evidence of non-compliance, or a regulator's requirement, the Controller may audit the Processor's compliance with this DPA. Routine audits are limited to once in any twelve (12) month period and require at least thirty (30) days' notice; the other cases need only reasonable notice. Every audit takes place during business hours, and is subject to confidentiality. It shall not extend to other customers' data. The Controller bears the cost unless the audit reveals a material breach.

11.3 A regulator with authority over the Controller may exercise equivalent rights where the law gives it that power.

12. Requests from authorities

12.1 If a public authority requests access to Personal Data, the Processor shall, where lawful:

- (a) notify the Controller promptly;
- (b) disclose only what is legally required; and
- (c) challenge requests it considers unlawful.

13. Liability, term and changes

13.1 Liability under this DPA is subject to the limitations of liability in the Agreement.

13.2 This DPA applies for as long as the Processor processes Personal Data for the Controller. Obligations on confidentiality, security, breach notification, deletion and audit evidence survive termination.

13.3 The Processor may publish a new version of this DPA on at least sixty (60) days' notice. A new version applies to a customer only as its Agreement permits. It never reduces the protection of Personal Data during the customer's current term without the customer's written agreement.

Annex 1 — Standard details of processing

These details apply unless the Controller's Processing Details state otherwise.

Item	Detail
Subject matter	Provision of Creatrix software and related implementation, configuration, integration, training and support services
Duration	The term of the Agreement, plus the retention periods in clause 10
Nature and purpose	Hosting, storage, structuring, validation, retrieval, use, transmission and deletion of Personal Data for the Controller's academic and institutional operations and its regulatory reporting
Data subjects	Applicants, students, alumni, faculty, staff, parents, guardians, sponsors and other individuals whose data the Controller records
Personal Data	Names and identifiers, including national identity and passport numbers where recorded; contact details; date of birth, gender and nationality; admission, enrolment, academic, attendance and graduation records; financial and fee records; employment and workload records; access credentials and usage logs
Sensitive Personal Data	Only where the Controller records it, for example disability or accommodation needs, health information for welfare purposes, or disciplinary records
Frequency	Continuous for the term of the Agreement

Annex 2 — Technical and organisational measures

Technical

- **Encryption:** AES-256 at rest and TLS in transit.
- **Access:** role-based access control and multi-factor authentication for all access to systems that process Personal Data.
- **Network:** firewalls, intrusion detection and prevention, and regular vulnerability scanning.
- **Isolation:** a dedicated production environment for each customer.

- **Backups:** continuous replication within the hosting region; database backups every four hours, retained for three days; daily backups retained for one month; weekly backups retained for three months; monthly snapshots retained for one year.
- **Disaster recovery:** recovery point objective of 12 hours and recovery time objective of 24 hours, tested at least every six months.
- **Logging:** access to and changes of Personal Data are logged and monitored.
- **Credentials:** third-party and regulator credentials are held in an encrypted secrets vault on a path restricted to the customer. They are never stored in configuration, email or tickets.

Organisational

- Documented data protection and information security policies, reviewed periodically.
- Data protection training for personnel with access to Personal Data.
- Confidentiality undertakings from employees, contractors and partners.
- Background checks for personnel with access to Personal Data, where the law permits.
- A documented incident response plan.
- Risk assessment of Sub-processors before engagement.
- Documented retention and secure disposal procedures.

Annex 3 — Jurisdiction-specific terms

Each section applies only where the named law applies to the processing.

United Arab Emirates.

- Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, and its implementing regulations once issued.
- For processing in the DIFC or ADGM, the data protection law of that free zone applies instead.
- The Parties shall agree any additional terms that the implementing regulations require for cross-border access.

Kingdom of Saudi Arabia.

- The Personal Data Protection Law (Royal Decree M/19 of 1443H) and its implementing regulations.
- Personal Data of customers hosted in Saudi Arabia remains in Saudi Arabia, subject to the transfer rules of that law.

Malaysia.

- The Personal Data Protection Act 2010, as amended, and the regulations and standards issued under it.
- The Processor supports the Controller's breach notification and data protection officer obligations under that Act.

India.

- The Digital Personal Data Protection Act, 2023, and the rules under it once in force.
- The Controller is the Data Fiduciary and the Processor is a Data Processor under that Act.

Singapore.

- The Personal Data Protection Act 2012.
- The Processor's obligations under this DPA include the protection, retention and breach notification obligations of a data intermediary under that Act.

European Union and United Kingdom.

- The EU General Data Protection Regulation or UK GDPR.
- This DPA is intended to meet Article 28. Where Personal Data is transferred outside the EEA or UK, the applicable Standard Contractual Clauses or UK Addendum apply and are incorporated by reference.

Other jurisdictions. Where another data protection law applies, the Processor shall comply with the obligations it places on processors. The Parties shall agree any additional terms that law requires.

Version history

Version	Effective	Summary
1.0	20 April 2026	First published version

Questions: dpo@anubavam.com · Security incidents: incidents@anubavam.com · Legal: legal@anubavam.com