



DCSAI Technologies

LEGAL DOCUMENT · v1.0 · MAY 2026

Data Processing Agreement

GDPR Article 28 · UK GDPR · DPDP · LGPD compliant

Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms part of the Master Services Agreement ("**Agreement**") between DCS AI Technologies L.L.C, a company incorporated in the United Arab Emirates with registered office at Office 40, Dubai Industrial City L.L.C, Saih Shuaib 3, Dubai, UAE, holder of Dubai Department of Economy & Tourism Commercial License No. 1624450 (Commercial Register No. 2862220, DCCI Membership No. 686532), with paid-up share capital of AED 250,000 ("**DCS**", "**Processor**"), and the customer entity identified in the order form ("**Customer**", "**Controller**"), each a "**Party**" and together the "**Parties**".

This DPA reflects the Parties' agreement with regard to the Processing of Personal Data by DCS on behalf of the Customer in connection with the Services. It is designed to satisfy the requirements of Article 28 of Regulation (EU) 2016/679 (the "**GDPR**"), the UK GDPR, the Indian Digital Personal Data Protection Act 2023 ("**DPDP**"), the Brazilian Lei Geral de Proteção de Dados ("**LGPD**"), and the California Consumer Privacy Act ("**CCPA**").

In case of conflict between this DPA and the Agreement, this DPA prevails with respect to matters relating to the Processing of Personal Data.

1. Definitions

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party.

"Authorised Sub-processor" means each sub-processor listed in Schedule 3 and any other sub-processor engaged by DCS in accordance with Clause 6.

"Customer Personal Data" means Personal Data Processed by DCS on behalf of the Customer pursuant to or in connection with the Agreement.

"Data Subject" has the meaning given in Article 4(1) GDPR.

"International Transfer" means a transfer of Personal Data to a country outside the European Economic Area that is not the subject of an adequacy decision by the European Commission.

"Personal Data" has the meaning given in Article 4(1) GDPR.

"Personal Data Breach" has the meaning given in Article 4(12) GDPR.

"Processing" has the meaning given in Article 4(2) GDPR and "Process" shall be interpreted accordingly.

"Services" means the products and services made available by DCS to the Customer under the Agreement (including DCS Platform, Compute, Storage, OS, Sovereign, and any other DCS-branded offering).

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses approved by the European Commission Decision 2021/914 of 4 June 2021, as may be updated from time to time.

"Sub-processor" means any entity engaged by DCS or its Affiliates to Process Customer Personal Data on its behalf.

2. Scope and Roles

2.1 This DPA applies to the Processing of Customer Personal Data by DCS to provide the Services.

2.2 The Parties acknowledge that:

- (a)** The Customer is the Controller of the Customer Personal Data.
- (b)** DCS is the Processor and may engage Sub-processors in accordance with this DPA.
- (c)** Each Party shall comply with the obligations applicable to it under the GDPR and other applicable data protection laws.

2.3 The details of the Processing (subject matter, duration, nature, purpose, types of Personal Data, and categories of Data Subjects) are set out in Schedule 1.

3. Processor Obligations

DCS shall:

- 3.1** Process Customer Personal Data only on documented instructions from the Customer, including with regard to International Transfers, unless required by EU or Member State law to which DCS is subject. In such a case, DCS shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.
- 3.2** Ensure that persons authorised to Process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- 3.3** Implement the technical and organisational measures set out in Schedule 2 to ensure a level of security appropriate to the risk.
- 3.4** Respect the conditions referred to in Clauses 6 and 7 for engaging Sub-processors and assist the Customer with International Transfers.
- 3.5** Taking into account the nature of the Processing, assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights.
- 3.6** Assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of Processing and the information available to DCS.
- 3.7** At the choice of the Customer, delete or return all Customer Personal Data after the end of the provision of services relating to Processing, and delete existing copies unless EU or Member State law requires storage of the Personal Data.
- 3.8** Make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, in accordance with Clause 8.

4. Controller Obligations

The Customer shall:

- 4.1** Comply with all applicable data protection laws in respect of its Processing of Personal Data and any Processing instructions it issues to DCS.
- 4.2** Ensure that it has all necessary rights, consents, and notices in place to enable lawful transfer of the Customer Personal Data to DCS for the duration and purposes of the Agreement.
- 4.3** Be solely responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which it acquired the Personal Data.
- 4.4** Communicate to Data Subjects, when required, the information referred to in Articles 13 and 14 GDPR.

5. Security

5.1 DCS shall implement the technical and organisational measures set out in Schedule 2 to ensure a level of security appropriate to the risk of Processing.

5.2 In assessing the appropriate level of security, DCS shall take into account in particular:

- the state of the art and the costs of implementation;
- the nature, scope, context, and purposes of Processing;
- the varying likelihood and severity of risks for the rights and freedoms of natural persons;
- the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

5.3 DCS's security measures are independently audited annually under SOC 2 Type II and ISO/IEC 27001. Current audit reports are available to the Customer under NDA.

6. Sub-processors

6.1 The Customer hereby grants DCS general authorisation to engage Sub-processors for the performance of the Services, subject to the conditions set out in this Clause 6.

6.2 An up-to-date list of Authorised Sub-processors is maintained at dcsai.ai/sub-processors and is reproduced in Schedule 3 as at the Effective Date.

6.3 DCS shall give the Customer at least 30 days' prior written notice (via the email address on file or via the Customer dashboard) of any intended addition or replacement of Sub-processors. The Customer may object on reasonable grounds related to data protection within 30 days. If the Parties cannot resolve the objection, the Customer may terminate the affected Service without penalty.

6.4 Where DCS engages a Sub-processor, DCS shall:

(a) enter into a written contract with the Sub-processor that imposes data protection obligations substantially similar to those set out in this DPA;

(b) remain fully liable to the Customer for the performance of the Sub-processor's obligations.

7. International Transfers

7.1 DCS may transfer Customer Personal Data to recipients outside the EEA, the UK, or the relevant jurisdiction, only:

- (a)** to a country in respect of which an adequacy decision has been issued by the relevant authority; or
- (b)** pursuant to the Standard Contractual Clauses (as incorporated into this DPA by reference); or
- (c)** pursuant to another lawful mechanism for International Transfers permitted under applicable data protection laws.

7.2 The Parties hereby enter into the Standard Contractual Clauses, which shall apply to International Transfers made by DCS to a Sub-processor located in a third country. The modular SCCs are incorporated by reference; the relevant module (typically Module 2: Controller to Processor or Module 3: Processor to Processor) shall apply based on the role of the Sub-processor.

7.3 Schedule 4 sets out the parameters required by the SCCs (parties, transfer details, technical and organisational measures, competent supervisory authority).

8. Audits

8.1 DCS shall make available to the Customer the information reasonably necessary to demonstrate compliance with its obligations under this DPA.

8.2 At the Customer's written request, and no more than once per calendar year (except where required following a Personal Data Breach), DCS shall:

- (a) provide a copy of its most recent SOC 2 Type II and ISO/IEC 27001 reports; and
- (b) respond to a reasonable written audit questionnaire within 30 days.

8.3 On-site audits are available to enterprise-tier Customers, subject to (i) reasonable advance notice (at least 60 days), (ii) the auditor signing DCS's standard non-disclosure agreement, (iii) the audit being conducted during normal business hours and in a manner that does not disrupt DCS's operations, and (iv) the Customer bearing the cost of the audit.

9. Personal Data Breach

9.1 DCS shall notify the Customer without undue delay and in any event within 72 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data.

9.2 The notification shall include, to the extent then known:

- a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- the name and contact details of DCS's Data Protection Officer;
- a description of the likely consequences of the Personal Data Breach;
- a description of the measures taken or proposed to address the Personal Data Breach.

9.3 DCS shall cooperate with the Customer and take such reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation, and remediation of any Personal Data Breach.

10. Term and Termination

10.1 This DPA shall remain in effect for the duration of the Agreement.

10.2 On termination of the Agreement, DCS shall (at the Customer's election) delete or return all Customer Personal Data to the Customer within 30 days, save to the extent that EU or Member State law requires storage of the Personal Data.

10.3 Cryptographic erasure (as described in the DCS Storage whitepaper) satisfies the deletion obligation under Clause 10.2 with respect to Customer Personal Data held in DCS Storage.

11. Liability

11.1 Each Party's liability under or in connection with this DPA is governed by the limitation of liability provisions of the Agreement.

11.2 Nothing in this DPA limits either Party's liability for: (i) gross negligence or wilful misconduct; (ii) breach of confidentiality; or (iii) liability that cannot be excluded under applicable law.

12. Governing Law and Jurisdiction

12.1 This DPA is governed by the laws of England and Wales unless the Agreement specifies a different governing law, in which case that law applies.

12.2 Disputes arising out of or in connection with this DPA shall be resolved in accordance with the dispute resolution provisions of the Agreement.

Schedule 1 — Processing Details

Subject matter · Provision of the DCS Services to the Customer under the Agreement.

Duration · The term of the Agreement, plus any period of post-termination retention permitted under Clause 10.

Nature and purpose · Processing necessary to provide the Services, including: hosting, storage, transmission, computation, indexing, analytics, audit logging, support, and billing.

Types of Personal Data · Identification data (name, email); authentication data (hashed credentials); usage data (logs, telemetry, audit receipts); any Personal Data submitted by the Customer or end-users via the Services.

Categories of Data Subjects · Customer's personnel; Customer's end-users; any individual whose Personal Data is submitted to the Services by the Customer.

Retention · Customer Personal Data is retained for the term of the Agreement and deleted within 30 days of termination, subject to legal retention requirements.

Schedule 2 — Technical and Organisational Measures

DCS implements the following measures to ensure a level of security appropriate to the risk:

Pseudonymisation and encryption of personal data

- All Personal Data is encrypted at rest using AES-256-GCM with per-tenant data encryption keys held in hardware security modules (FIPS 140-2 Level 3).
- All Personal Data in transit is encrypted using TLS 1.3 with forward secrecy.
- Per-tenant encryption keys can be destroyed on Customer request, rendering ciphertext unrecoverable (cryptographic erasure).

Confidentiality, integrity, availability and resilience

- Multi-region replication: data is replicated across at least 3 warm storage providers and up to 7 cold Filecoin storage providers in different jurisdictions.
- Tamper-evidence: every system action emits a signed receipt (DCS Standards R+1/R+2). Tampering with any record breaks the cryptographic chain.
- Access logging: all access to Customer Personal Data is logged with the actor identity, timestamp, and purpose.
- Background checks: all DCS personnel with access to production systems undergo standard employment background checks.

Ability to restore availability and access to personal data

- Recovery Point Objective (RPO): 5 minutes for hot data; 1 hour for warm data.
- Recovery Time Objective (RTO): 30 minutes for hot data; 4 hours for warm data.
- Quarterly disaster recovery exercises with documented results.

Regular testing, assessing, and evaluating

- SOC 2 Type II audit annually by an independent third-party auditor.
- ISO/IEC 27001 certification renewed annually.
- Penetration testing semi-annually by an independent security firm.
- Continuous vulnerability scanning of all production infrastructure.

Schedule 3 — Authorised Sub-processors

The following are the Authorised Sub-processors as at the Effective Date. The current list is maintained at dcsai.ai/sub-processors.

Sub-processor	Purpose	Region	GDPR mechanism
Amazon Web Services	Hot storage (S3) + EC2 compute	EU + US	SCCs Mod. 2
Cloudflare	CDN + edge caching + DNS + R2	Global	SCCs Mod. 2
Stripe Inc.	Payment processing + Connect payouts	US	SCCs Mod. 2
Anthropic PBC	LLM inference (Claude family)	US	SCCs Mod. 3
OpenAI LLC	LLM inference (GPT family)	US	SCCs Mod. 3
Supabase Inc.	Auth + Postgres-managed	EU + US	SCCs Mod. 2
Backblaze Inc.	B2 cold storage	US	SCCs Mod. 2
Filecoin SPs (various)	7-replica cold backup	Global	Per-SP terms
Lighthouse Storage Inc.	Filecoin upload broker	India	SCCs Mod. 2 + DPDP
Resend	Transactional email	US	SCCs Mod. 2
Vercel Inc.	Frontend hosting (Cloudflare Pages fallback)	Global	SCCs Mod. 2
Railway Corp.	Backend service hosting	US	SCCs Mod. 2

Schedule 4 — Standard Contractual Clauses (SCC Annexes)

Annex I.A — List of Parties

Data Exporter (Controller): The Customer entity identified in the Order Form.

Data Importer (Processor): DCS AI Technologies L.L.C, registered office Office 40, Dubai Industrial City L.L.C, Saih Shuaib 3, Dubai, UAE. Contact: legal@dcsai.ai. DPO: dpo@dcsai.ai.

Annex I.B — Description of Transfer

See Schedule 1 above.

Annex I.C — Competent Supervisory Authority

The supervisory authority of the EU Member State in which the Customer is established. If the Customer is established outside the EU, the Irish Data Protection Commission shall be the competent supervisory authority.

Annex II — Technical and Organisational Measures

See Schedule 2 above.

Annex III — List of Sub-processors

See Schedule 3 above.

Signatures

This DPA is effective as of the date last signed below.

For DCS AI Technologies L.L.C

For Customer

Signature: _____

Signature: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

This DPA template is published under CC BY 4.0. Counterparties may incorporate it by reference into their Agreement with DCS, or sign an executed copy. Questions: legal@dcsai.ai.