



INTERNATIONAL DATA TRANSFER ADDENDUM (IDTA)

Including Standard Contractual Clauses (SCCs) and Other Applicable Transfer Mechanisms

For International Transfers of Personal Data. Applicable where required by relevant data protection and privacy laws.

Applicability: This International Data Transfer Addendum incorporates Standard Contractual Clauses (SCCs) where required by applicable law. Where SCCs are not the appropriate transfer mechanism, the parties shall rely on another lawful transfer mechanism recognized by the applicable jurisdiction.

SECTION 1: PARTIES

DATA EXPORTER

Company Name:

Address:

Contact Person:

Email:

Role: Controller / Processor

DATA IMPORTER

Company Name: Virideed Technologies

Address: Plot 504 Steve Amadi Street,
WorksLayout, Owerri, Imo State, Nigeria.

Contact Person: Chidi Ejike

Title: Founder

Email: support@virideed.com

Role: Processor

SECTION 2: TRANSFER DETAILS

Categories of Data Subjects

End-users of the Data Exporter's AI systems whose inputs and outputs are processed for compliance auditing purposes.

Categories of Personal Data Transferred

- Names, email addresses, user IDs
- AI input/output content
- Session identifiers
- IP addresses and location data

- Compliance and audit records

Sensitive Data Transferred

Sensitive personal data and special categories of personal data (where applicable) as defined under applicable data protection laws, processed only as necessary to provide the contracted services.

Frequency of Transfer

Continuous (real-time per API call).

Nature of Processing

Automated compliance auditing, risk scoring, PII detection, regulatory mapping, and audit trail generation.

Purpose of Transfer

To provide AI governance, observability, and compliance services as contracted between the parties.

Duration of Processing

- As specified in the Data Retention Policy
- Audit logs: Logs are retained in accordance with applicable limitation periods, legal retention obligations, regulatory requirements, contractual obligations, and Virideed's data retention policies.
- Training data: 90 days (where applicable).
- Raw PII: Retained only as part of audit records and retained in accordance with applicable limitation periods, legal retention obligations, regulatory requirements, contractual obligations, and Virideed's data retention policies.

Transfer Impact Assessment

This is the responsibility of the Data Exporter. Virideed Technologies provides the technical and organizational measures documented in Appendix A to support the Data Exporter's Transfer Impact Assessment.

SECTION 3: COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be determined by the Data Exporter's place of establishment and the applicable data protection legislation in their jurisdiction.

SECTION 4: OBLIGATIONS OF THE DATA IMPORTER (Virideed)

4.1 Purpose Limitation

The Data Importer shall process personal data only for the purposes described in Section 2.

4.2 Confidentiality

The Data Importer shall ensure that persons authorized to process the personal data have committed themselves to confidentiality.

4.3 Security

The Data Importer shall implement appropriate technical and organizational measures:

- Encryption at rest: AES-256
- Encryption in transit: TLS 1.3
- Infrastructure: Google Cloud infrastructure certified against SOC 2 Type II and ISO 27001 standards and configured to support applicable privacy and data protection requirements.
- Access permissions are assigned according to authorized user roles and business requirements.
- Access logging: Per-user and per-session audit logging. Shared audit records may be made available through customer-controlled sharing mechanisms where configured by the customer.

4.4 Sub-processing

The Data Importer engages Google Cloud Platform as a sub-processor. Any additional sub-processors shall be communicated to the Data Exporter. The Data Importer shall maintain an up-to-date list of sub-processors and make such list available to the Data Exporter upon request.

4.5 Data Subject Rights

The Data Importer shall assist the Data Exporter in responding to data subject requests.

4.6 Breach Notification

The Data Importer shall notify the Data Exporter without undue delay upon becoming aware of a personal data breach.

4.7 Deletion or Return

Upon termination of services, the Data Importer shall delete all personal data, subject to retention requirements specified in Section 2.

SECTION 5: SIGNATURES

**For and on behalf of the Data Importer
(Virideed Technologies):**

Signature:  _____

Name: Chidi Ejike

Title: Founder

Date: 2026-06-16

For and on behalf of the Data Exporter:

Signature: _____

Name: _____

Title: _____

Date: _____

APPENDIX A: TECHNICAL AND ORGANIZATIONAL MEASURES

Measure	Details
Encryption at rest	AES-256
Encryption in transit	TLS 1.3
Key management	Customer-held key or Virideed Google Cloud KMS
Infrastructure certifications	Google Cloud infrastructure certified against SOC 2 Type II and ISO 27001 standards and configured to support applicable privacy and data protection requirements.
Access control	Role-based, least privilege
Access logging	Per-user, per-session
Data residency	Data is processed and stored in Google Cloud infrastructure located in the United States (currently us-central1). Personal data transferred from other jurisdictions may be subject to international data transfer requirements and is protected through applicable lawful transfer mechanisms. Customers acknowledge that personal data may be transferred to and processed in the United States in connection with the provision of the services.
Transfer mechanism	Personal data is transferred using the lawful transfer mechanism required by the applicable jurisdiction, including where applicable: • European Commission Standard Contractual Clauses (SCCs) (Module 2 Controller-to-Processor and/or Module 3 Processor-to-Processor) • UK International Data Transfer Agreement (IDTA) or UK Addendum • EU-US Data Privacy Framework (DPF), where available and applicable • Other legally recognized transfer mechanisms approved by the applicable data protection authority These mechanisms are supplemented by encryption, access controls, audit logging, customer-managed encryption keys (where configured), and Google Cloud security controls.
Supplementary Measure	Technical and organizational measures including encryption, access controls, audit logging, Google Cloud security controls, and customer-held cryptographic keys where configured.
Additional Transfer Mechanisms	Where applicable, other lawful transfer mechanisms recognized by the relevant data protection authority may be used.

APPENDIX B: SUB-PROCESSORS

Sub-processor	Purpose	Location
Google Cloud Platform	Cloud infrastructure (Cloud Run, Firestore, KMS)	United States (us-central1)

This document is pre-signed by Virideed Technologies.

Download, complete your company details, sign, and retain for your compliance records.

For questions, contact: support@virideed.com