Data Processing Agreement

Between SkillsOS (“Processor”) and Customer Institution (“Controller”)

Effective Date: Upon execution of Service Agreement

---

1. Definitions

“Personal Data” means any information relating to an identified or identifiable natural person, including but not limited to student education records, faculty information, and institutional data.

“Processing” means any operation performed on Personal Data, including collection, storage, modification, retrieval, disclosure, and deletion.

“Data Subject” means the individual to whom Personal Data relates.

“Sub-processor” means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

“Security Incident” means any unauthorized access, acquisition, use, or disclosure of Personal Data.

---

2. Scope of Processing

2.1 Purpose

The Processor shall process Personal Data only for the following purposes:

- Providing the SkillsOS platform services as described in the Service Agreement
- Maintaining and improving platform functionality
- Providing customer support
- Ensuring platform security and compliance

2.2 Categories of Data

Category	Data Elements
Student Data	Name, email, student ID, enrollment data, credentials earned
Faculty Data	Name, email, department, courses taught
Institutional Data	Programs, curricula, organizational structure
Usage Data	Platform interactions, analytics, audit logs

2.3 Duration

Processing shall continue for the duration of the Service Agreement plus any retention period required by law or specified in Section 8.

---

3. Processor Obligations

3.1 Compliance

The Processor shall:

- Process Personal Data only on documented instructions from the Controller
- Ensure personnel are bound by confidentiality obligations
- Implement appropriate technical and organizational security measures
- Assist the Controller in responding to Data Subject requests
- Delete or return Personal Data upon termination of services

3.2 Security Measures

The Processor implements the following security measures:

Category	Measures
Encryption	AES-256 at rest, TLS 1.3 in transit
Access Control	RBAC, MFA, SSO integration
Monitoring	$^{24}/_{7}$ security monitoring, audit logging
Backup	Daily encrypted backups, geographic redundancy
Testing	Annual penetration testing, vulnerability scanning

3.3 Sub-processors

The Processor shall:

- Maintain a list of approved Sub-processors (Exhibit A)
- Notify the Controller of any intended changes to Sub-processors
- Ensure Sub-processors are bound by equivalent data protection obligations
- Remain liable for Sub-processor compliance

---

4. Controller Obligations

The Controller shall:

- Ensure lawful basis for processing Personal Data
- Provide clear instructions to the Processor
- Obtain necessary consents from Data Subjects where required
- Notify the Processor of any Data Subject requests or complaints

---

5. Data Subject Rights

5.1 Supported Rights

The Processor shall assist the Controller in fulfilling requests for:

- Access to Personal Data
- Rectification of inaccurate data
- Erasure of Personal Data (“right to be forgotten”)
- Restriction of processing
- Data portability
- Objection to processing

5.2 Response Timeline

The Processor shall respond to Controller requests within:

- **Standard requests**: 10 business days
- **Urgent requests**: 48 hours

---

6. Security Incident Response

6.1 Notification

The Processor shall notify the Controller of any Security Incident:

- **Initial notification**: Within 24 hours of discovery
- **Detailed report**: Within 72 hours

6.2 Notification Contents

Security Incident notifications shall include:

- Nature of the incident
- Categories and approximate number of affected Data Subjects
- Likely consequences
- Measures taken or proposed to address the incident

6.3 Cooperation

The Processor shall cooperate with the Controller in:

- Investigating the incident
- Mitigating adverse effects
- Fulfilling regulatory notification obligations

---

7. Audits and Assessments

7.1 Audit Rights

The Controller may:

- Request and review SOC 2 Type II audit reports
- Request completion of security questionnaires (e.g., HECVAT)
- Conduct or commission third-party audits with reasonable notice

7.2 Processor Cooperation

The Processor shall:

- Provide requested documentation within 10 business days
- Facilitate on-site audits with 30 days advance notice
- Address identified deficiencies within agreed timelines

---

8. Data Retention and Deletion

8.1 Retention Period

Personal Data shall be retained for:

- **Active accounts**: Duration of Service Agreement
- **Inactive accounts**: 90 days after last activity

- **Audit logs**: 7 years (or as required by law)

8.2 Deletion

Upon termination of the Service Agreement:

- The Processor shall delete or return all Personal Data within 30 days
- The Controller may request a certificate of deletion
- Backup copies shall be deleted within 90 days

---

9. International Data Transfers

9.1 Transfer Mechanisms

For transfers outside the originating jurisdiction, the Processor employs:

- Standard Contractual Clauses (SCCs) approved by relevant authorities
- Binding Corporate Rules where applicable
- Adequacy decisions where available

9.2 Additional Safeguards

The Processor implements supplementary measures including:

- Encryption of data in transit and at rest
- Access controls limiting data access by jurisdiction
- Regular assessment of transfer mechanism validity

---

10. FERPA Compliance (US Educational Institutions)

10.1 School Official Designation

The Processor is designated as a “school official” under FERPA with legitimate educational interest in accessing education records to provide contracted services.

10.2 FERPA Commitments

The Processor shall:

- Use education records only for authorized purposes
- Not disclose education records except as permitted
- Maintain appropriate security for education records
- Return or destroy education records upon request

---

11. Liability and Indemnification

11.1 Processor Liability

The Processor shall be liable for damages caused by processing that:

- Violates this Agreement
- Violates applicable data protection laws
- Results from Processor negligence or willful misconduct

11.2 Limitation

Liability limitations in the Service Agreement apply to this DPA, except for:

- Willful misconduct
- Gross negligence
- Violations of data protection laws

---

12. Term and Termination

12.1 Term

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

12.2 Survival

Sections 6 (Security Incidents), 7 (Audits), 8 (Retention/Deletion), and 11 (Liability) shall survive termination.

---

13. Amendments

This DPA may be amended:

- By mutual written agreement
- By the Processor to reflect changes in applicable law (with 30 days notice)

Exhibit A: Approved Sub-processors

Sub-processor	Purpose	Location
Vercel Inc.	Application hosting	United States
Supabase Inc.	Database services	United States
Amazon Web Services	File storage	United States
SendGrid (Twilio)	Email delivery	United States
Stripe Inc.	Payment processing	United States
OpenAI	AI processing	United States

Last updated: December 2024

Signatures

For SkillsOS (Processor):

Name: _____

Title: _____

Date: _____

Signature: _____

For Customer Institution (Controller):

Name: _____

Title: _____

Date: _____

Signature: _____
