



# DATA PROCESSING AGREEMENT

AJAEQ Inc.

|                                                     |   |
|-----------------------------------------------------|---|
| RECITALS.....                                       | 3 |
| 1. DEFINITIONS.....                                 | 3 |
| 2. SCOPE AND PURPOSE OF PROCESSING.....             | 3 |
| 2.1 Nature of Processing.....                       | 3 |
| 2.2 Categories of Personal Data.....                | 4 |
| 2.3 Special Categories of Data.....                 | 4 |
| 2.4 Duration of Processing.....                     | 4 |
| 3. CONTROLLER OBLIGATIONS.....                      | 4 |
| 3.1 Lawful Basis.....                               | 4 |
| 3.2 Data Subject Notification.....                  | 4 |
| 3.3 Accuracy.....                                   | 4 |
| 3.4 Instructions.....                               | 4 |
| 3.5 Compliance.....                                 | 4 |
| 4. PROCESSOR OBLIGATIONS.....                       | 5 |
| 4.1 Processing in Accordance with Instructions..... | 5 |
| 4.2 Confidentiality.....                            | 5 |
| 4.3 Security Measures.....                          | 5 |
| 4.4 Sub-processors.....                             | 5 |
| 4.5 Data Subject Rights Assistance.....             | 5 |
| 4.6 Data Protection Impact Assessments.....         | 5 |
| 4.7 Audit Rights.....                               | 5 |
| 5. SECURITY INCIDENT NOTIFICATION.....              | 6 |
| 5.1 Notification Obligation.....                    | 6 |
| 5.2 Content of Notification.....                    | 6 |
| 5.3 Cooperation.....                                | 6 |
| 5.4 Controller Notification Obligations.....        | 6 |
| 6. INTERNATIONAL DATA TRANSFERS.....                | 6 |
| 6.1 Data Location.....                              | 6 |
| 6.2 Transfer Safeguards.....                        | 6 |
| 6.3 Nigerian Data Protection Compliance.....        | 6 |
| 7. DATA RETENTION AND DELETION.....                 | 6 |
| 7.1 Retention During Service Term.....              | 6 |

|                                              |   |
|----------------------------------------------|---|
| 7.2 Return or Deletion Upon Termination..... | 7 |
| 7.3 Retention Exceptions.....                | 7 |
| 7.4 Certification Records.....               | 7 |
| 8. REPORTING AND ACCESS.....                 | 7 |
| 8.1 Controller Access to Data.....           | 7 |
| 8.2 Individual User Data.....                | 7 |
| 9. LIABILITY AND INDEMNIFICATION.....        | 7 |
| 9.1 Processor Liability.....                 | 7 |
| 9.2 Controller Liability.....                | 7 |
| 10. TERM AND TERMINATION.....                | 7 |
| 10.1 Term.....                               | 7 |
| 10.2 Termination.....                        | 7 |
| 11. GOVERNING LAW.....                       | 8 |
| 12. GENERAL PROVISIONS.....                  | 8 |
| 13. CONTACT INFORMATION.....                 | 8 |

## RECITALS

This Data Processing Agreement ("DPA" or "Agreement") is entered into between AJAEQ Inc. ("AJAEQ," "Processor," "Service Provider," "we," "us," or "our"), a corporation incorporated under the laws of the State of Delaware, United States of America, with its registered address at 2810 N Church St #701434, Wilmington, DE 19802, and the contracting institution, enterprise organization, or individual user ("Controller," "Client," or "you") identified in the applicable service agreement, subscription, or institutional contract.

WHEREAS, AJAEQ provides cybersecurity education, simulation, and professional development services through its platform; WHEREAS, in the course of providing such services, AJAEQ may process personal data of students, employees, or other individuals on behalf of the Controller; WHEREAS, both parties wish to establish the terms under which such data processing shall occur in compliance with applicable data protection laws; NOW THEREFORE, in consideration of the mutual obligations set forth herein, the parties agree as follows:

## 1. DEFINITIONS

**"Applicable Data Protection Law"** means all applicable laws and regulations relating to the processing of personal data, including but not limited to: the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA); the Nigeria Data Protection Act 2023 (NDPA); the Nigeria Data Protection Regulation (NDPR); and the General Data Protection Regulation (EU) 2016/679 (GDPR) where applicable.

**"Controller"** means the entity that determines the purposes and means of processing Personal Data, being the institutional client, university, or enterprise organization entering into a Service Agreement with AJAEQ.

**"Data Subject"** means any identified or identifiable natural person whose Personal Data is processed under this Agreement, including but not limited to enrolled students, employees, and authorized users.

**"Personal Data"** means any information relating to an identified or identifiable Data Subject.

**"Processing"** means any operation or set of operations performed on Personal Data, whether by automated means.

**"Processor"** means AJAEQ Inc., which processes Personal Data on behalf of the Controller.

**"Security Incident"** means any confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed under this Agreement.

**"Sub-processor"** means any third party engaged by AJAEQ to process Personal Data in connection with the Services.

## 2. SCOPE AND PURPOSE OF PROCESSING

### 2.1 Nature of Processing

AJAEQ processes Personal Data as a Processor on behalf of the Controller solely for the purpose of providing the Services described in the applicable Service Agreement, including:

- (a) Creating and maintaining user accounts for Data Subjects authorized by the Controller.
- (b) Providing access to educational content, career path curricula, and learning resources.
- (c) Operating Laboratory environments and simulation sessions for Data Subjects.
- (d) Recording progress, performance metrics, and completion data for enrolled Data Subjects.
- (e) Issuing certifications upon completion of required program components.
- (f) Providing reporting and analytics to the Controller regarding Data Subjects' platform engagement and performance.

(g) Processing payments where applicable.

## **2.2 Categories of Personal Data**

(a) Identification data: full name, username, email address.

(b) Authentication data: hashed and salted passwords, multi-factor authentication tokens.

(c) Profile data: country of residence, date of birth, institutional affiliation.

(d) Learning data: course progress, exercise completions, assessment scores, certification status, simulation session history.

(e) Technical data: IP address, device identifiers, browser type, operating system.

(f) Laboratory Session Data: commands executed, network interactions, and system activity within AJAEQ-hosted simulation environments.

(g) Payment data: processed exclusively by Stripe, Inc.; no raw payment card data is stored on AJAEQ systems.

(h) Communications: support requests, feedback submissions, and platform correspondence.

## **2.3 Special Categories of Data**

AJAEQ does not intentionally collect or process special categories of Personal Data (including data revealing racial or ethnic origin, political opinions, religious beliefs, health data, or biometric data for identification purposes) unless specifically required by the Service Agreement and subject to additional safeguards to be agreed upon in writing.

## **2.4 Duration of Processing**

AJAEQ will process Personal Data for the duration of the Service Agreement and for such additional periods as required by applicable law or as specified in our Privacy Policy's data retention schedule.

# **3. CONTROLLER OBLIGATIONS**

## **3.1 Lawful Basis**

The Controller has a valid and lawful basis under Applicable Data Protection Law for disclosing Personal Data to AJAEQ and for instructing AJAEQ to process such data as described in this Agreement.

## **3.2 Data Subject Notification**

The Controller has provided or will provide all necessary notices to Data Subjects regarding the processing of their Personal Data by AJAEQ, including disclosure of AJAEQ's role as Processor.

## **3.3 Accuracy**

The Controller is responsible for ensuring the accuracy and completeness of Personal Data provided to AJAEQ. AJAEQ shall not be liable for processing inaccurate data provided by the Controller.

## **3.4 Instructions**

The Controller's instructions to AJAEQ regarding the processing of Personal Data shall be lawful, specific, and documented. AJAEQ will process Personal Data solely in accordance with such documented instructions, except where required by applicable law to do otherwise.

## **3.5 Compliance**

The Controller shall comply with all Applicable Data Protection Laws in its capacity as Controller, including any obligations relating to data subject rights, breach notification, and data protection impact assessments.

## **4. PROCESSOR OBLIGATIONS**

### **4.1 Processing in Accordance with Instructions**

AJAEQ will process Personal Data only on documented instructions from the Controller, as set forth in this Agreement and the applicable Service Agreement, except where processing is required by applicable law.

### **4.2 Confidentiality**

AJAEQ will ensure that all personnel authorized to process Personal Data are subject to appropriate confidentiality obligations and have received adequate data protection training.

### **4.3 Security Measures**

AJAEQ will implement and maintain appropriate technical and organizational measures to protect Personal Data, including:

- (a) Encryption of Personal Data in transit using TLS 1.3.
- (b) Encryption of Personal Data at rest using industry-standard encryption.
- (c) Access controls limiting Personal Data access to authorized personnel on a need-to-know basis.
- (d) Multi-factor authentication for administrative access to systems processing Personal Data.
- (e) Regular security assessments of our platform and infrastructure.
- (f) Incident response procedures for Security Incidents.
- (g) Physical security measures at data center facilities operated by Amazon Web Services (AWS).

### **4.4 Sub-processors**

The Controller hereby grants AJAEQ general authorization to engage Sub-processors. Current approved Sub-processors include:

- Amazon Web Services (AWS):** Cloud infrastructure, compute, storage, database — United States (primary).
- Stripe, Inc.:** Payment processing — United States.
- PostHog:** Product analytics — United States.

AJAEQ will notify the Controller of any intended addition or replacement of Sub-processors, providing the Controller an opportunity to object within fourteen (14) days of such notification.

### **4.5 Data Subject Rights Assistance**

AJAEQ will assist the Controller in responding to Data Subject requests to exercise rights under Applicable Data Protection Law, and will promptly notify the Controller upon receiving any Data Subject request relating to data processed on behalf of the Controller.

### **4.6 Data Protection Impact Assessments**

Where required by Applicable Data Protection Law, AJAEQ will provide reasonable assistance to the Controller in conducting data protection impact assessments.

### **4.7 Audit Rights**

Upon the Controller's written request and with reasonable notice (not less than thirty (30) days), AJAEQ will make available to the Controller such information as is reasonably necessary to demonstrate compliance with this Agreement.

## **5. SECURITY INCIDENT NOTIFICATION**

### **5.1 Notification Obligation**

In the event of a confirmed Security Incident affecting Personal Data processed under this Agreement, AJAEQ will notify the Controller without undue delay and in any event within seventy-two (72) hours of becoming aware of the incident.

### **5.2 Content of Notification**

Security Incident notifications will include: (a) a description of the nature of the incident; (b) contact details of AJAEQ's data protection point of contact; (c) a description of the likely consequences; and (d) a description of the measures taken or proposed to address the incident.

### **5.3 Cooperation**

AJAEQ will cooperate with the Controller in investigating Security Incidents and in meeting the Controller's obligations to notify Data Subjects and regulatory authorities.

### **5.4 Controller Notification Obligations**

Where notification to regulatory authorities or Data Subjects is required, such notification is the responsibility of the Controller. AJAEQ will provide reasonable assistance.

## **6. INTERNATIONAL DATA TRANSFERS**

### **6.1 Data Location**

Personal Data processed under this Agreement is primarily stored and processed on Amazon Web Services infrastructure located in the United States.

### **6.2 Transfer Safeguards**

Where Personal Data is transferred from Nigeria, the European Economic Area, the United Kingdom, or other jurisdictions with data transfer restrictions to the United States or other countries, AJAEQ will implement appropriate transfer safeguards in accordance with Applicable Data Protection Law, including standard contractual clauses as approved by relevant supervisory authorities.

### **6.3 Nigerian Data Protection Compliance**

For Personal Data of Nigerian Data Subjects, AJAEQ shall comply with the requirements of the Nigeria Data Protection Act 2023 and the Nigeria Data Protection Regulation.

## **7. DATA RETENTION AND DELETION**

### **7.1 Retention During Service Term**

AJAEQ will retain Personal Data for the duration of the Service Agreement and for such additional periods as specified in AJAEQ's Privacy Policy or required by applicable law.

## **7.2 Return or Deletion Upon Termination**

Upon termination of the Service Agreement, AJAEQ will, at the Controller's election: (a) return all Personal Data to the Controller in a structured, commonly used, machine-readable format within thirty (30) days; or (b) securely delete or destroy all Personal Data, with confirmation of deletion provided to the Controller within thirty (30) days.

## **7.3 Retention Exceptions**

AJAEQ may retain Personal Data for longer periods where required by applicable law, including for legal proceedings, regulatory compliance, or audit purposes.

## **7.4 Certification Records**

Certification records issued to individual users will be retained indefinitely to enable lifetime certification verification, regardless of account or service termination.

# **8. REPORTING AND ACCESS**

## **8.1 Controller Access to Data**

The Controller may access aggregated performance and progress data for enrolled Data Subjects through the reporting features of the AJAEQ administrative portal, to the extent included in the applicable Service Agreement.

## **8.2 Individual User Data**

Individual user data will be provided to the Controller only as specified in the Service Agreement and to the extent consistent with applicable data protection law and AJAEQ's obligations to individual Data Subjects.

# **9. LIABILITY AND INDEMNIFICATION**

## **9.1 Processor Liability**

AJAEQ's liability under this Agreement is subject to the limitations set forth in the Terms of Use. AJAEQ shall be liable for damages caused by processing where it has not complied with obligations under this Agreement specifically directed to Processors under Applicable Data Protection Law.

## **9.2 Controller Liability**

The Controller shall indemnify, defend, and hold harmless AJAEQ from and against any claims, liabilities, damages, losses, costs, and expenses arising from: (a) the Controller's failure to comply with its obligations as a Controller; (b) the Controller's provision of inaccurate or unlawfully obtained Personal Data to AJAEQ; or (c) the Controller's instructions to AJAEQ that violate Applicable Data Protection Law.

# **10. TERM AND TERMINATION**

## **10.1 Term**

This Agreement is effective from the date the Controller first accesses AJAEQ's Services or executes a Service Agreement, and continues for the duration of the Service Agreement.

## **10.2 Termination**

This Agreement automatically terminates upon termination of the applicable Service Agreement. Obligations regarding Security Incidents, data deletion, and record retention shall survive termination.

## **11. GOVERNING LAW**

This Agreement shall be governed by the laws of the State of Delaware, United States of America. For Nigerian institutional clients, nothing in this Agreement limits the application of the Nigeria Data Protection Act 2023 or associated regulations.

## **12. GENERAL PROVISIONS**

In the event of any conflict between this Agreement and the Terms of Use or Privacy Policy, this Agreement shall prevail with respect to data processing matters. AJAEQ reserves the right to modify this Agreement where required by changes in Applicable Data Protection Law, with thirty (30) days' written notice to affected Controllers.

## **13. CONTACT INFORMATION**

Data Protection Contact:

Oluwatimilehin N. Obalade

AJAEQ Inc., 2810 N Church St #701434, Wilmington, DE 19802

Email: [office@ajaeq.com](mailto:office@ajaeq.com)