DATA PROCESSING AGREEMENT

BETWEEN

ELYCROX GLOBAL LTD

("CONTROLLER")

AND

XYZ

("PROCESSOR")

IN RESPECT OF:

THE PROCESSING OF PERSONAL DATA ON BEHALF OF THE CONTROLLER.

PREPARED BY:

GODWIN OJEH ESQ.
MUHAMMED ADAM & ASSOCIATES
Flat 2, South Lake Homes
1, Ugochukwu Orji
StreetOff Lekki-Epe
Expressway, Lekki, Lagos.
adam@muhammedadam.com,
07081093303

THIS DATA PROCESSING AGREEMENT ("the **Agreement"** or **"DPA"**) is made this ___ day of _____ 2026

BETWEEN

ELYCROX GLOBAL LTD., a company duly incorporated under the laws of the Federal Republic of Nigeria with its registered office at No. 87, Aiyegbami Estate, Asadam Road, Ilorin, Kwara State, Nigeria (hereinafter referred to as the **"Controller"**, which expression shall where the context admits include successors, affiliates, and permitted assigns)

AND

XYZ of _____ (hereinafter referred to as the **"Processor"**, which expression shall where the context admits include permitted successors, subcontractors approved under this Agreement, and authorised personnel).

The **Controller** and **Processor** may each be referred to as a **"Party"** and collectively as the **"Parties".**

WHEREAS

A. The Controller operates digital entertainment, competition, audience engagement, production, content, technology, payment, registration, verification, and platform services including activities associated with the FURY™ ecosystem.

B. The Processor provides services which may involve receiving, accessing, collecting, storing, analysing, transmitting, hosting, verifying, processing, supporting, securing, or otherwise handling Personal Data on behalf of the Controller.

C. The Parties wish to define their respective obligations regarding the lawful and secure processing of Personal Data.

D. This Agreement supplements and forms part of any underlying services agreement, vendor agreement, procurement agreement, technology agreement, implementation agreement, consulting agreement, statement of work, or commercial engagement.

NOW IT IS AGREED as follows:

1. **PURPOSE AND APPLICATION**

1.1 This Agreement governs the Processor's processing of Personal Data on behalf of the Controller.

1.2 This Agreement applies wherever Personal Data is collected, stored, transmitted, viewed, analysed, hosted, transferred, accessed, deleted, matched, verified, exported, archived, monitored, or otherwise processed.

1.3 This Agreement applies regardless of whether Personal Data is processed within Nigeria, cross-border, through cloud infrastructure, through subcontractors, through APIs, through production systems, through integrated software, or through manual processes.

1.4 This Agreement shall prevail over conflicting data processing provisions unless expressly agreed otherwise in writing.

1.5 Processing activities governed by this Agreement may include website hosting, platform development, cloud infrastructure, payment processing, identity verification, KYC operations, email delivery, customer support, analytics, marketing systems, security monitoring, content moderation, production operations, audience engagement systems, and competition administration.

2. DEFINITIONS

2.1 In this Agreement:

"Applicable Data Protection Laws" means all laws, regulations, directives, regulatory guidance, binding codes, standards, and legal requirements governing privacy, Personal Data, electronic communications, cybersecurity, information governance, and data processing applicable to the Services and Processing activities including, where applicable:

i. the Nigeria Data Protection Act, 2023 and regulations, directives, implementation frameworks, and guidance issued by the Nigeria Data Protection Commission;
ii. applicable data protection and privacy laws of jurisdictions in which Data Subjects are located;
iii. laws governing international transfers of Personal Data;
iv. applicable sector-specific obligations affecting identity verification, payments, digital services, communications, and platform operations.

References to Applicable Data Protection Laws shall include any amendment, replacement, consolidation, reenactment, subsidiary instrument, or successor legislation.

"Controller" means the Party determining purposes and means of processing.

"Processor" means the Party processing Personal Data on behalf of the Controller.

"Data Subject" means an identified or identifiable natural person.

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

"Sensitive Personal Data" means Personal Data requiring heightened protection including identity information, government identifiers, biometric information, financial information, account credentials, verification records, and other protected categories recognised under Applicable Data Protection Laws.

"Processing" includes collection, storage, access, organisation, use, disclosure, transfer, deletion, retrieval, consultation, analysis, alteration, transmission, restriction, or destruction.

"Subprocessor" means any third party engaged by the Processor to carry out processing activities.

"Security Incident" means actual or suspected unauthorised access, loss, destruction, disclosure, alteration, misuse, compromise, interruption, exfiltration, or inability to access Personal Data.

"Services" means activities performed under the underlying commercial engagement.

3. PROCESSING DETAILS

3.1 Subject Matter

The Processor shall process Personal Data solely to perform the Services.

3.2 Nature of Processing

Processing may include hosting, storage, access management, transmission, identity verification, payment support, communications support, analytics processing, reporting, fraud monitoring, customer operations, and technical administration.

3.3 Categories of Data Subjects

Data Subjects may include users, contestants, voters, employees, contractors, vendors, investors, partners, website visitors, or support users.

3.4 Categories of Personal Data

Processing may involve identity information, contact information, account information, device information, payment records, verification records, transaction information, usage data, communications, technical logs and security information.

3.5 Sensitive Processing

Where Sensitive Personal Data is involved, the Processor shall apply enhanced protections appropriate to the nature and sensitivity of the information.

4. PROCESSOR OBLIGATIONS

4.1 The Processor shall process Personal Data only on documented instructions from the Controller.

4.2 The Processor shall not determine independent purposes of processing, sell Personal Data, share Personal Data for unrelated commercial purposes, combine datasets for independent profiling, use data to train artificial intelligence systems unless expressly authorized or retain unnecessary copies.

4.3 The Processor shall maintain policies, procedures, governance controls, and technical safeguards proportionate to processing risk.

4.4 The Processor shall immediately notify the Controller where an instruction appears unlawful or materially inconsistent with Applicable Data Protection Laws.

4.5 The Processor shall ensure that personnel accessing Personal Data receive appropriate training, operate under confidentiality obligations, have restricted access, and follow documented procedures.

5. CONTROLLER INSTRUCTIONS

5.1 Instructions may be provided through, the master services agreement, written operational instructions, platform documentation, approved workflows, ticketing systems, written correspondence, or authorised operational requests.

5.2 Instructions materially affecting risk, security, retention, transfers, or data subject rights shall be documented.

5.3 The Processor shall not materially change processing activities without written approval.

6. CONFIDENTIALITY AND PERSONNEL CONTROLS

6.1 The Processor shall ensure that all personnel authorised to process Personal Data are subject to legally enforceable obligations of confidentiality.

6.2 Access to Personal Data shall be limited strictly to individuals whose access is necessary for performance of the Services.

6.3 The Processor shall maintain internal access governance measures designed to ensure that access rights are granted, reviewed, modified, and withdrawn appropriately.

6.4 The Processor shall implement reasonable onboarding and offboarding procedures for personnel with access to Personal Data.

6.5 The Processor shall remain responsible for acts and omissions of its personnel and authorised representatives relating to processing activities.

6.6 The Processor shall implement measures designed to reduce risks arising from insider threats, unauthorised viewing, credential misuse, and improper disclosure.

7. INFORMATION SECURITY REQUIREMENTS

7.1 The Processor shall maintain appropriate administrative, organisational, technical, and physical safeguards designed to protect Personal Data.

7.2 Such safeguards shall take into account the nature of the Services, processing risks, state of available technology, implementation costs, volume and sensitivity of Personal Data, and risk to Data Subjects.

7.3 Security measures shall be designed to support confidentiality, integrity, availability, resilience, recoverability, and accountability.

7.4 Without limiting the Processor's obligations, security measures should reasonably address identity and access management, credential governance, least privilege access, logging and monitoring, environment segregation, secure transmission controls, vulnerability management, malware protection, backup procedures, secure deletion controls, business continuity, and incident response.

7.5 Encryption should be implemented where reasonably appropriate having regard to the sensitivity of Personal Data and operational context.

The Processor shall maintain documented security policies and review security practices periodically.

8. SUBPROCESSORS

8.1 The Processor shall not appoint a Subprocessor without prior written authorisation from the Controller.

8.2 Approval may be specific approval for identified Subprocessors, or general approval subject to advance notice procedures.

8.3 The Processor shall remain fully responsible for all processing activities performed by approved Subprocessors.

8.4 Before engaging a Subprocessor, the Processor shall conduct reasonable diligence appropriate to security posture, privacy controls, technical capability, compliance maturity, and operational reliability.

8.5 The Processor shall ensure that Subprocessors are bound by written obligations providing protection materially equivalent to this Agreement.

8.6 The Processor shall maintain an accurate and current list of approved Subprocessors and provide updates upon reasonable request.

8.7 Engagement of Subprocessors shall not reduce the Processor's accountability under this Agreement.

9. INTERNATIONAL DATA TRANSFERS

9.1 The Processor shall not transfer Personal Data outside approved jurisdictions except in accordance with Applicable Data Protection Laws and documented instructions.

9.2 Where cross-border transfers occur, the Processor shall implement safeguards appropriate to the transfer mechanism and applicable jurisdiction.

9.3 Such safeguards may include contractual transfer mechanisms, adequacy determinations, supplementary technical measures, organisational safeguards, or approved certification frameworks.

9.4 The Processor shall maintain reasonable visibility over locations where Personal Data is stored, hosted, replicated, accessed, or backed up.

9.5 The Processor shall notify the Controller before introducing material transfer changes which may significantly affect privacy or regulatory exposure.

10. SECURITY INCIDENT MANAGEMENT

10.1 The Processor shall maintain documented procedures for identifying, managing, investigating, containing, and remediating Security Incidents.

10.2 The Processor shall notify the Controller without undue delay after becoming aware of a Security Incident affecting Personal Data.

10.3 Initial notification shall include available information concerning, nature of the incident, categories of affected data, estimated scope, known or anticipated consequences, and initial remediation measures.

10.4 The Processor shall continue providing updates as additional information becomes available.

10.5 The Processor shall not communicate directly with affected Data Subjects, regulators, media organisations, or third parties regarding incidents unless authorised or legally required.

10.6 The Processor shall preserve relevant evidence and cooperate fully with investigations and remediation activities.

11. ASSISTANCE WITH DATA SUBJECT RIGHTS

11.1 Taking into account the nature of processing, the Processor shall assist the Controller in responding to requests relating to access, correction, deletion, restriction, objection, withdrawal of consent, portability, and complaints.

11.2 Where a request is received directly by the Processor, the Processor shall promptly notify the Controller unless prohibited by law.

11.3 The Processor shall not independently fulfil requests except where authorised.

11.4 Assistance shall be provided within commercially reasonable timelines.

12. ASSISTANCE WITH COMPLIANCE OBLIGATIONS

12.1 The Processor shall provide reasonable cooperation necessary to support the Controller's compliance obligations.

12.2 Assistance may include support relating to privacy assessments, risk evaluations, regulatory inquiries, security assessments, documentation requests, incident response, or data governance reviews.

12.3 The Processor shall make available information reasonably necessary to demonstrate compliance.

12.4 Without prejudice to broader obligations under Applicable Data Protection Laws, the Parties acknowledge that the Controller operates within Nigeria and may process Personal Data subject to the Nigeria Data Protection Act, 2023 (NDPA). Accordingly:

(a) the Processor shall implement measures reasonably necessary to support the Controller's compliance obligations under the NDPA;

(b) the Processor shall cooperate with reasonable requests connected with compliance reviews, privacy assessments, audit exercises, regulatory engagement, breach response, and lawful inquiries by the Nigeria Data Protection Commission;

(c) where Processing activities materially affect compliance obligations under Nigerian law, the Processor shall promptly notify the Controller and cooperate in implementing corrective measures.

13. PRIVACY IMPACT ASSESSMENTS

13.1 Where required under Applicable Data Protection Laws, the Processor shall provide reasonable information necessary to support privacy impact assessments or similar evaluations.

13.2 Cooperation shall be proportionate to the Services and processing risks.

13.3 Nothing in this clause requires disclosure of unrelated proprietary information.

14. RECORDS OF PROCESSING

14.1 The Processor shall maintain records reasonably necessary to demonstrate compliance with this Agreement.

14.2 Such records should reasonably describe processing activities, categories of Personal Data, categories of recipients, retention practices, security measures, and cross-border processing arrangements.

14.3 Records shall be retained for periods reasonably necessary to demonstrate compliance and satisfy legal obligations.

15. REGULATORY COOPERATION

15.1 The Processor shall notify the Controller promptly upon becoming aware of:

(a) regulatory requests;
(b) inspection notices;
(c) enforcement inquiries;
(d) governmental access requests;
(e) compliance investigations;
(f) inquiries, audits, notices, investigations, directives, complaints, enforcement actions, or requests issued by the Nigeria Data Protection Commission or any competent privacy regulator, where disclosure is legally permitted.

15.2 The Processor shall cooperate in good faith with lawful regulatory processes affecting Personal Data processed under this Agreement.

15.3 Unless legally prohibited, the Processor shall provide reasonable opportunity for the Controller to participate in responses affecting its data.

16. AUDIT AND COMPLIANCE VERIFICATION

16.1 The Controller shall have the right, acting reasonably and upon prior notice, to verify the Processor's compliance with this Agreement.

16.2 Verification may occur through written compliance questionnaires, security attestations, document reviews, certification evidence, virtual reviews, independent audit reports, and reasonable inspection procedures.

16.3 Physical inspections shall only occur where reasonably necessary having regard to the nature of processing and subject to security and confidentiality safeguards.

16.4 The Processor shall provide reasonable cooperation necessary to demonstrate compliance.

16.5 Audit rights shall not be exercised in a manner intended to access unrelated confidential information, disrupt operations, or expose information relating to other customers.

16.6 Where independent audit reports are available and reasonably sufficient, the Controller may rely upon such reports instead of conducting additional audits.

17. RETENTION, RETURN, AND DELETION OF PERSONAL DATA

17.1 The Processor shall not retain Personal Data longer than necessary for the Services or applicable legal obligations.

17.2 Upon completion, expiry, termination, or written request, the Controller may instruct the Processor to return Personal Data, delete Personal Data, destroy stored copies, export data in a structured format.

17.3 The Processor shall complete such actions within a commercially reasonable period unless retention is legally required.

17.4 Where deletion occurs, the Processor shall provide written confirmation upon request.

17.5 Backup copies maintained through routine operational systems may remain subject to restricted access and continuing confidentiality obligations until overwritten or deleted in accordance with standard retention cycles.

17.6 The Processor shall not continue using retained Personal Data for analytics, commercial activities, training systems, benchmarking, product development, or unrelated purposes.

18. BUSINESS CONTINUITY AND RESILIENCE

18.1 The Processor shall maintain appropriate business continuity and recovery measures proportionate to the Services.

18.2 Such measures should be reasonably designed to support continuity of processing and minimise disruption.

18.3 The Processor shall maintain procedures addressing service interruption, loss of availability, system failure, disaster recovery, restoration activities, and incident escalation.

18.4 Material disruptions affecting Personal Data shall be communicated promptly to the Controller.

19. USE OF AUTOMATED TOOLS, AI, AND ANALYTICS

19.1 The Processor shall not use Personal Data for development, training, testing, tuning, or optimisation of artificial intelligence, machine learning, automated decision systems, behavioural profiling systems, or internal product enhancement activities unless expressly authorised in writing.

19.2 The Processor shall not create derivative datasets from Controller Personal Data except where required to perform the Services.

19.3 Any authorised analytics activities shall remain limited to the documented processing purposes.

19.4 Aggregation or anonymisation activities shall not permit re-identification of individuals.

19.5 The Processor shall maintain reasonable safeguards designed to prevent unintended exposure through automated processing environments.

20. LIABILITY

20.1 Each Party shall remain responsible for its own acts, omissions, personnel, and compliance obligations.

20.2 The Processor shall be responsible for losses directly arising from processing outside instructions, security failures attributable to the Processor, unauthorised disclosure, unapproved Subprocessor activity, or material breach of this Agreement.

20.3 The Controller shall remain responsible for lawfulness of collection, lawful instructions, privacy notices, consent mechanisms where applicable, and determination of processing purposes.

20.4 Nothing in this Agreement excludes liability for fraud, wilful misconduct, unlawful processing, intentional misuse of Personal Data, or gross negligence.

21. INDEMNITY

21.1 Subject to applicable law, the Processor shall indemnify and hold harmless the Controller from losses directly arising from material breach of this Agreement by the Processor.

21.2 Recoverable losses may include reasonable costs associated with incident management, regulatory response, investigation, remediation, legal advisers, notification obligations, and technical recovery.

21.3 Each Party shall take reasonable steps to mitigate recoverable losses.

22. TERM AND TERMINATION

22.1 This Agreement shall become effective on execution.

22.2 This Agreement shall continue for so long as the Processor processes Personal Data on behalf of the Controller.

22.3 Termination of the underlying commercial agreement shall not automatically extinguish obligations relating to Personal Data.

22.4 The Controller may suspend or terminate processing instructions where continued processing would create material legal, regulatory, security, or operational risk.

22.5 Upon termination or expiry of this Agreement, or upon cessation of the Services for any reason, the Processor shall immediately cease all Processing activities except to the extent retention or continued Processing is required under Applicable Laws.

22.6 Subject to the Controller's written instructions, the Processor shall within **thirty (30) days** after termination:

(a) securely return Personal Data to the Controller in a structured, commonly used, and commercially reasonable format;

(b) securely delete or permanently destroy all copies of Personal Data under its control;

(c) discontinue all active access, synchronisation, indexing, replication, and operational use of such Personal Data;

(d) provide written certification confirming completion of return or deletion activities where reasonably requested.

22.7 Where Applicable Laws require retention of Personal Data after termination:

(a) the Processor may retain only the minimum information legally required;

(b) retained information shall remain subject to confidentiality and security obligations under this Agreement;

(c) retained information shall not be used for any independent operational, commercial, analytics, profiling, training, development, or marketing purpose.

22.8 For a reasonable transition period following termination, not exceeding **sixty (60) days** unless otherwise agreed in writing, the Processor shall provide reasonable cooperation to facilitate orderly migration, continuity of operations, and secure transfer of Personal Data and associated processing activities.

22.9 Termination of this Agreement shall not relieve the Processor of obligations relating to confidentiality, information security, regulatory cooperation, incident notification, deletion requirements, audit support where reasonably required in connection with prior Processing activities, cross-border transfer safeguards, and liability for prior acts or omissions.

23. Survival of Rights

23.1 Termination of this Agreement shall be without prejudice to rights, remedies, liabilities, indemnities, investigations, audit rights, or obligations which accrued before the effective date of termination.

23.2 Obligations relating to confidentiality, security, retention, regulatory cooperation, audit, liability, indemnity, deletion obligations and cross-border safeguards, shall survive termination to the extent necessary to give effect to their purpose.

24. NOTICES

25.1 Notices under this Agreement shall be in writing.

25.2 Notices may be delivered personally, by recognised courier, or electronically to the designated addresses of the Parties.

25.3 Notices shall be deemed received on delivery where personally delivered, two business days after courier dispatch or on transmission where sent electronically without failure notification.

24. GOVERNING LAW AND DISPUTE RESOLUTION

25.4 This Agreement shall be governed by and construed in accordance with the laws of the Federal Republic of Nigeria.

25.5 Any dispute arising out of or relating to this Agreement shall first be addressed through good faith discussions.

25.6 Where the dispute remains unresolved within **fourteen (14) days** after written notification, the matter shall be referred to mediation administered through the Lagos Multi Door Courthouse.

25.7 If mediation does not resolve the dispute within **thirty (30) days** after commencement, either Party may refer the matter to a court of competent jurisdiction in Lagos State, Nigeria.

25.8 Nothing in this clause prevents the Company from seeking urgent protective relief where necessary to preserve rights, protect intellectual property, prevent misuse, maintain operational integrity, prevent fraud, enforce Platform rules, or comply with legal obligations.

26 GENERAL PROVISIONS

26.1 This Agreement constitutes the entire understanding between the Parties with respect to the subject matter herein. It supersedes all prior agreements, negotiations, and understandings whether written or oral.

26.2 No amendment to this Agreement shall be valid unless made in writing and signed by both Parties.

26.3 Failure by either Party to enforce any provision shall not constitute a waiver of that provision. Any waiver must be in writing.

26.4 If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect. The Parties shall replace such invalid provision with a valid one that reflects the original intent as closely as possible.

26.5 Each Party shall execute all documents and take all steps necessary to give full effect to this Agreement.

26.6 Provisions relating to confidentiality, intellectual property, transfer restrictions, dispute resolution, and any other provisions intended by their nature to survive shall remain in effect notwithstanding termination.

26.7 This Agreement may be executed electronically and in counterparts, each of which shall be deemed an original.

IN WITNESS WHEREOF the Parties have executed this Agreement on the date first above written.

THE COMMON SEAL of the within named Company **"ELYCROX GLOBAL LTD"** is hereby affixed in the presence of:

_____
Director

SIGNED, by the within-named **"PROCESSOR"**

_____
XYZ

IN THE PRESENCE OF:
Name: _____

Address: _____

Occupation: _____

Signature: _____

SCHEDULE 1
PROCESSING DETAILS

Controller: _____

Processor: _____

Services: _____

Processing Purpose: _____

Categories of Data Subjects: _____

Categories of Personal Data: _____

Retention Period: _____

Approved Transfer Locations: _____

Approved Subprocessors: _____

SCHEDULE 2
SECURITY REQUIREMENTS

To be completed depending on vendor category and risk profile.

SCHEDULE 3
APPROVED SUBPROCESSOR REGISTER

To be updated from time to time.

SCHEDULE 4
INCIDENT CONTACT DETAILS

Controller Contact: _____

Processor Contact: _____

Incident Escalation Email: _____

Incident Escalation Number: _____