Data Processing Agreement — Frontier Interactions Ltd

1. Parties

This Data Processing Agreement ("**Agreement**") forms part of the Service Contract ("**Principal Agreement**") between:

Frontier Interactions Ltd
(the "**Company**" or "**Data Controller**")

and

_____
(the "**Data Processor**")
(together the "**Parties**")

2. Background

(A) The Company acts as a Data Controller under the UK GDPR.
(B) The Company wishes to subcontract certain Services involving the processing of personal data to the Data Processor.
(C) The Parties wish to ensure compliance with Regulation (EU) 2016/679 and the UK Data Protection Act 2018.
(D) This Agreement sets out their respective rights and obligations.

3. Definitions

Unless otherwise defined herein, the following terms have the meanings set out in the UK GDPR:

- "Personal Data", "Processing", "Controller", "Processor", "Data Subject", "Personal Data Breach", "Supervisory Authority", and other related terms shall have the meanings assigned in the UK GDPR.
- "Company Personal Data" means any Personal Data processed by the Processor on behalf of the Company.
- "Subprocessor" means any person or entity appointed by the Processor to process Personal Data on behalf of the Company.
- "Data Protection Laws" means the UK GDPR, the Data Protection Act 2018, and any other applicable privacy laws.
- "Services" means the services provided by the Processor under the Principal Agreement.

4. Processing of Data

The Processor shall:
- process Company Personal Data only on documented instructions from the Company;
- comply with all applicable Data Protection Laws;
- ensure all persons authorized to process Personal Data are bound by confidentiality obligations.

The Company instructs the Processor to process Personal Data as necessary for the performance of the Services.

5. Security Measures

The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Article 32 of the UK GDPR, including (as applicable) encryption, pseudonymization, access control, and data integrity monitoring.

Frontier Interactions Ltd enforces secure access control at all levels of its infrastructure:
1. Developer and Admin Accounts – All internal systems (GitHub, Vercel, Render, Supabase, Elevenlabs, OpenAI) require Multi-Factor Authentication (MFA). Shared credentials are prohibited.
2. SDK & API Layer – The SDK does not provide end-user authentication. It relies on company-level credentials to obtain a secure access token from the backend during initialization. Subsequent requests are authorized through token-based validation and company-specific keys, ensuring that only verified client environments can interact with the backend.
3. Least-Privilege Access – Access rights are granted strictly based on job role and necessity. Production databases are access-controlled using Row Level Security (RLS).
4. Key & Secret Management – Secrets are managed using encrypted environment variables on Render and Vercel, rotated periodically and upon staff role changes.
5. Audit & Monitoring – Access logs are monitored; privilege reviews are conducted quarterly.

6. Subprocessing

The Processor shall not appoint any Subprocessor without the prior written authorization of the Company. Where authorization is granted, the Processor shall ensure equivalent data protection obligations are imposed on the Subprocessor.

The Company's current list of authorized subprocessors is available at:
https://docs.heykulu.ai/docs/security/sub-processors
and may be updated from time to time with prior written notice to the Company.

7. Data Subject Rights

The Processor shall assist the Company in responding to requests to exercise Data Subject rights, including access, rectification, restriction, erasure, and portability.

8. Personal Data Breach Notification

The Processor shall notify the Company without undue delay after becoming aware of a Personal Data Breach and shall cooperate to investigate and mitigate the incident.

9. Data Protection Impact Assessments

The Processor shall assist the Company with data protection impact assessments and consultations with supervisory authorities where required under Articles 35 and 36 of the UK GDPR.

10. Return or Deletion of Data

Upon termination of the Services, the Processor shall delete or return all Company Personal Data within 10 business days, unless retention is required by law. Backups shall be purged within the next backup cycle.

11. Audit and Compliance

The Processor shall make available to the Company all information necessary to demonstrate compliance with this Agreement and allow for audits by the Company or its designated auditor, no more than once per year.

12. International Data Transfers

No transfer of Personal Data outside the UK or EEA shall occur without the Company's prior written consent. Where such transfers are required, the Parties shall rely on the applicable UK International Data Transfer Addendum or EU Standard Contractual Clauses. Copies or signed templates of such Addendum or Clauses are available upon request.

13. Confidentiality

Each Party shall treat as confidential all information received from the other Party in connection with this Agreement, except where disclosure is required by law or where information is already public.

14. Contacts

All data protection and security-related communications shall be directed to: support@heykulu.ai

15. Notices

All notices under this Agreement must be in writing and delivered personally or sent by email to the addresses set out above (or such other address as either Party may later notify).

16. Governing Law and Jurisdiction

This Agreement is governed by the laws of England and Wales. Any dispute shall be submitted to the exclusive jurisdiction of the courts of England and Wales.

Schedule 1 – Data Processing Details

Purpose of Processing: Provision of software onboarding and automation services
Nature of Processing: Storage, transmission, and structured analysis of customer data
Type of Personal Data: Names, emails, user activity logs, recorded interactions
Data Subjects: Company employees, customers, and authorized users
Duration: For the duration of the Principal Agreement and lawful retention period
Retention: active lifecycle of the Principal Agreement + up to 90 days for backups, unless earlier deletion is requested or required by law.

Schedule 2 – Technical & Organizational Measures

The Processor shall implement, at minimum, the following security controls to ensure an appropriate level of protection:

- Secure access control – Enforced across all internal systems (GitHub, Vercel, Render, Supabase, Google Workspace).
- Encryption in transit (TLS 1.2+) and at rest (AES-256) – Applied to all data flows and storage layers.

- Data segregation per company account (RLS) – Enforced at the database level via Supabase Row-Level Security.
- Regular vulnerability scanning and patching – Core dependencies and infrastructure components are monitored and patched as needed.
- Backup and recovery procedures – Automated backups with secure storage and periodic verification.
- Information security framework – Frontier Interactions Ltd is currently implementing its information security management system aligned with ISO 27001.

Signatures

Frontier Interactions Ltd
Signature: _____
Name: _____
Title: _____
Date: _____

Company _____
Signature: _____
Name: _____
Title: _____
Date: _____

Return signed copies to: support@heykulu.ai