

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 “**Data Processor**”)

and

(the “**Data Controller**”)
(together the “**Parties**”)

2. Background

- (A) The Data Controller acts as a Data Controller under applicable data protection laws.
- (B) The Data Controller uses Frontier Interactions’ platform, and related services, which involve the Data Processor processing personal data on the Data Controller’s behalf.
- (C) The Parties wish to ensure that such processing complies with the UK GDPR, EU GDPR (as applicable), 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.
- “Controller Personal Data” means any Personal Data processed by the Processor on behalf of the Controller.
- “Sub-processor” means any person or entity appointed by the Processor to process Personal Data on behalf of the Controller.
- “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 Controller Personal Data only on documented instructions from the Controller;
- comply with all applicable Data Protection Laws;
- ensure all persons authorized to process Personal Data are bound by confidentiality obligations.

The Controller instructs the Processor to process Personal Data as necessary for providing the Services, including meeting initialization, workflow tracking, and onboarding analytics. No special-category data (Article 9, UK GDPR) is intended to be processed. Where the Processor considers that an instruction infringes Data Protection Laws, it shall promptly inform the Controller.

5. Security Measures

The Processor shall implement technical and organizational measures appropriate to the risk, including encryption in transit and at rest, access control, and regular review of access privileges.

6. Subprocessing

The Controller authorizes the use of Sub-processors as reasonably necessary for the Services.

The current list is published at <https://docs.heykulu.ai/docs/security/privacy> and may be updated from time to time. The Processor shall ensure all Sub-processors are bound by written data protection terms no less protective than this Agreement and remains fully liable for their performance.

7. Data Subject Rights

The Processor shall assist the Controller 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 Controller without undue delay upon becoming aware of a Personal Data Breach.

9. Data Protection Impact Assessments

The Processor shall assist the Controller with DPIAs and supervisory-authority consultations where required (Articles 35–36, UK/EU GDPR), limited to the Processor’s processing activities and available information.

10. Return or Deletion of Data

Upon termination or written request, the Processor shall delete Controller Personal Data unless retention is required by law.

11. Audit and Compliance

The Processor shall provide reasonable information to demonstrate compliance with this Agreement upon written request.

12. International Data Transfers

Personal Data may be transferred outside the UK or EEA under the UK International Data Transfer Addendum (IDTA) or EU Standard Contractual Clauses (SCCs), as applicable.

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 shall be in writing and sent by email to the contact addresses

provided by the Parties.

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.

Signatures

Frontier Interactions Ltd

Signature: _____

Name: _____

Title: _____

Date: _____

_____ (Data Controller)

Signature: _____

Name: _____

Title: _____

Date: _____

Return signed copies to: support@heykulu.ai