QUALZAI INC.

DATA PROCESSING ADDENDUM (Enterprise Version)

Effective Date: [Insert Date]

This Data Processing Addendum ("DPA") forms part of the Terms of Use or applicable agreement ("Agreement") between:

QualzAI Inc. ("Processor")
and
Customer ("Controller").

This DPA applies where Processor processes Personal Data on behalf of Controller subject to Applicable Data Protection Law.

---

1. DEFINITIONS

"Applicable Data Protection Law" means all applicable data protection laws, including Regulation (EU) 2016/679 ("GDPR").

"Personal Data," "Processing," "Controller," "Processor," and **"Data Subject"** have the meanings set forth in GDPR.

"Subprocessor" means any third party engaged by Processor to process Personal Data.

"Standard Contractual Clauses" or **"SCCs"** means the European Commission Implementing Decision (EU) 2021/914.

2. ROLE OF THE PARTIES

2.1 Controller determines the purposes and means of processing Personal Data.

2.2 Processor processes Personal Data solely:

- On documented instructions from Controller;
- For purposes defined in the Agreement;
- In compliance with Applicable Data Protection Law.

2.3 Processor shall immediately inform Controller if instructions violate Applicable Data Protection Law.

3. DETAILS OF PROCESSING (GDPR Article 28(3))

The subject matter, nature, and purpose of processing are described in Annex I.

4. PROCESSOR OBLIGATIONS

Processor shall:

- **(a)** Process Personal Data only on documented instructions;
- **(b)** Ensure personnel are bound by confidentiality;
- **(c)** Implement appropriate technical and organizational measures (see Annex II);
- **(d)** Assist Controller in fulfilling GDPR Articles 12–23 (Data Subject rights);
- **(e)** Assist Controller in ensuring compliance with Articles 32–36 (Security, DPIAs, prior consultation);
- **(f)** Delete or return Personal Data upon termination (see Section 10);
- **(g)** Make available information necessary to demonstrate compliance.

5. SECURITY MEASURES (GDPR Article 32)

Processor implements technical and organizational measures appropriate to the risk, including:

- Encryption in transit (TLS 1.2+)
- Logical segregation of customer data
- Role-based access control
- Multi-factor authentication for administrative access
- Secure cloud infrastructure environments
- Logging and monitoring mechanisms
- Regular review of access privileges
- Incident response procedures
- Secure development lifecycle practices

Full details are described in Annex II.

Processor may update measures provided protection is not materially diminished.

6. SUBPROCESSORS

6.1 General Authorization

Controller grants Processor general authorization to appoint Subprocessors.

6.2 Subprocessor Safeguards

Processor shall:

- Enter written agreements imposing data protection obligations equivalent to this DPA;
- Remain liable for Subprocessor compliance.

6.3 Subprocessor List

A current list of Subprocessors will be provided upon request.

6.4 Objection Right

Controller may object to a new Subprocessor on reasonable data protection grounds within 15 days of notification.

7. INTERNATIONAL DATA TRANSFERS

7.1 Transfers outside the EEA shall be subject to:

- Standard Contractual Clauses (Module 2 – Controller to Processor); or
- An adequacy decision; or
- Another valid transfer mechanism.

7.2 The SCCs are incorporated by reference and deemed executed between the parties.

For SCC purposes:

Role	Party
Data Exporter	Controller
Data Importer	Processor
Governing law	Ireland (or other EU Member State)

Processor does not guarantee data localization unless separately agreed.

8. DATA SUBJECT RIGHTS

Processor shall:

- Promptly notify Controller of requests received;
- Not respond directly unless required by law;
- Provide reasonable assistance in fulfilling requests.

9. PERSONAL DATA BREACH

9.1 Processor shall notify Controller without undue delay and, where feasible, within **72 hours** of becoming aware of a Personal Data Breach affecting Controller data.

9.2 Notification shall include:

- Nature of the breach;
- Categories of affected data;
- Likely consequences;
- Measures taken or proposed.

Processor shall cooperate with Controller in remediation.

10. DATA RETENTION & DELETION

Upon termination of Services, Processor shall, at Controller's choice:

- Delete Personal Data; or
- Return Personal Data.

Deletion from backups may occur in accordance with standard retention cycles not exceeding **30 days** unless legally required otherwise.

11. AUDIT RIGHTS

11.1 Processor shall make available documentation demonstrating compliance.

11.2 Controller may conduct an audit:

- Upon 30 days' written notice;
- During normal business hours;
- No more than once annually;
- At Controller's expense.

Audits shall not unreasonably disrupt operations.

12. LIABILITY

Liability under this DPA is subject to limitations in the Agreement, except where not permitted under Applicable Data Protection Law.

13. TERM

This DPA remains effective as long as Processor processes Personal Data on behalf of Controller.

ANNEX I – DETAILS OF PROCESSING

Field	Description
Subject Matter	Provision of qualitative research and AI-powered analysis services
Duration	For the duration of the Agreement
Nature and Purpose	Hosting, storage, analysis, and processing of research data uploaded by Controller

Categories of Data Subjects:

- Research participants
- Customer employees
- Platform users

Types of Personal Data:

- Names
- Contact information
- Interview responses
- Survey responses
- Audio files
- Text data
- Metadata

ANNEX II – TECHNICAL AND ORGANIZATIONAL MEASURES

Processor maintains measures including:

Infrastructure Security

- Secure cloud hosting environments
- Network segmentation
- Firewall protection

Access Controls

- Role-based access control
- Multi-factor authentication
- Logging and monitoring

Encryption

- TLS encryption in transit
- Encryption at rest where supported by infrastructure

Organizational Measures

- Confidentiality agreements
- Limited personnel access
- Security awareness practices

Incident Management

- Documented incident response process
- Breach notification procedures