Data Processing Agreement

(DPA)

This Data Processing Agreement forms part of the Master Services Agreement between the parties for the provision of AIRA Analytics services.

BETWEEN:

Data Controller ("Client") [Client Company Name]
[Address]
[Country]

AND:

Data Processor Spry Insights FZCO
Business Center, Al Shmookh Building
UAQ Free Trade Zone, Umm Al Quwain, UAE

Version	1.0
Effective Date	[Date]
GDPR Compliant	Yes

RECITALS

WHEREAS, the Client wishes to engage the Processor to provide data analytics services through the AIRA Analytics platform, which may involve the processing of personal data;

WHEREAS, the parties wish to ensure that such processing is conducted in compliance with applicable data protection laws, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("GDPR");

NOW, THEREFORE, the parties agree as follows:

Article 1: Definitions

1.1 **"Personal Data"** means any information relating to an identified or identifiable natural person as defined in Article 4(1) of the GDPR.

1.2 **"Processing"** means any operation performed on Personal Data, including collection, storage, analysis, and deletion.

1.3 **"Data Subject"** means the identified or identifiable natural person to whom the Personal Data relates.

1.4 **"Sub-processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Client.

1.5 **"Data Breach"** means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

1.6 **"Services"** means the AIRA Analytics platform and related data analytics services provided by the Processor.

Article 2: Scope and Purpose of Processing

2.1 The Processor shall process Personal Data only for the purpose of providing the Services as described in the Master Services Agreement and in accordance with the Client's documented instructions.

2.2 The categories of Personal Data and Data Subjects are set out in Annex A of this Agreement.

2.3 The duration of processing shall be for the term of the Master Services Agreement unless otherwise specified in writing.

Article 3: Processor Obligations

The Processor agrees to:

3.1 Process Personal Data only on documented instructions from the Client, unless required by law;

3.2 Ensure that persons authorized to process Personal Data have committed to confidentiality;

3.3 Implement appropriate technical and organizational security measures as described in Annex B;

3.4 Respect the conditions for engaging Sub-processors as set out in Article 5;

3.5 Assist the Client in responding to Data Subject requests;

3.6 Assist the Client in ensuring compliance with Articles 32-36 of the GDPR;

3.7 Delete or return all Personal Data upon termination of Services, at the Client's choice;

3.8 Make available all information necessary to demonstrate compliance and allow for audits.

Article 4: Client Obligations

The Client warrants and agrees that:

4.1 It has obtained all necessary consents and legal bases for the processing of Personal Data;

4.2 It shall provide documented instructions for processing that comply with applicable law;

4.3 It shall notify the Processor without undue delay of any changes affecting the processing;

4.4 It is responsible for the accuracy, quality, and legality of Personal Data provided to the Processor.

Article 5: Sub-processors

5.1 The Client provides general authorization for the Processor to engage Sub-processors, subject to the conditions in this Article.

5.2 The Processor shall maintain an up-to-date list of Sub-processors, available upon request.

5.3 The Processor shall notify the Client of any intended changes to Sub-processors at least 30 days in advance, allowing the Client to object.

5.4 The Processor shall ensure that Sub-processors are bound by data protection obligations no less protective than those in this Agreement.

5.5 The Processor remains fully liable for the acts and omissions of its Sub-processors.

Article 6: Security Measures

6.1 The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- Encryption of Personal Data in transit and at rest;
- Measures to ensure ongoing confidentiality, integrity, availability, and resilience;
- Regular testing and evaluation of security measures;
- Processes for restoring availability and access in the event of an incident.

6.2 Detailed security measures are set out in the Data Security Policy (Annex B).

Article 7: Data Breach Notification

7.1 The Processor shall notify the Client without undue delay, and in any event within 24 hours, upon becoming aware of a Data Breach affecting Client Personal Data.

7.2 Such notification shall include, to the extent possible:

- A description of the nature of the breach;
- The categories and approximate number of Data Subjects and records concerned;
- The likely consequences of the breach;
- Measures taken or proposed to address the breach.

Article 8: Data Subject Rights

8.1 The Processor shall assist the Client in fulfilling its obligation to respond to Data Subject requests, including requests for access, rectification, erasure, restriction, portability, and objection.

8.2 If the Processor receives a request from a Data Subject directly, it shall promptly notify the Client and shall not respond without the Client's instructions, unless required by law.

Article 9: International Data Transfers

9.1 The Processor shall not transfer Personal Data to a country outside the European Economic Area (EEA) without ensuring appropriate safeguards are in place.

9.2 Appropriate safeguards may include:

- Transfer to a country with an adequacy decision;
- Standard Contractual Clauses approved by the European Commission;
- Binding Corporate Rules;
- Other lawful transfer mechanisms under applicable law.

Article 10: Audit Rights

10.1 The Processor shall make available to the Client all information necessary to demonstrate compliance with this Agreement and applicable data protection law.

10.2 The Client may conduct audits, including inspections, upon reasonable notice. Such audits shall be conducted during normal business hours and shall not unreasonably disrupt the Processor's operations.

10.3 The Client may accept third-party audit reports (e.g., SOC 2) as evidence of compliance.

Article 11: Data Return and Deletion

11.1 Upon termination or expiry of the Services, the Processor shall, at the Client's election:

- Return all Personal Data to the Client in a commonly used format; and/or
- Delete all Personal Data and certify such deletion in writing.

11.2 Deletion shall be completed within 30 days of termination, unless longer retention is required by applicable law.

Article 12: Liability

12.1 Each party shall be liable for damages caused by processing that infringes applicable data protection law or this Agreement.

12.2 The Processor shall be liable for damage caused by processing only where it has not complied with its obligations under this Agreement or applicable law, or has acted outside or contrary to the Client's lawful instructions.

Article 13: General Provisions

13.1 This Agreement shall be governed by the laws of the United Arab Emirates, without regard to conflict of law principles.

13.2 In the event of conflict between this Agreement and the Master Services Agreement, this Agreement shall prevail with respect to data protection matters.

13.3 This Agreement may be amended only in writing signed by both parties.

SIGNATURES

IN WITNESS WHEREOF, the parties have executed this Data Processing Agreement as of the date last signed below.

FOR THE CLIENT:	FOR THE PROCESSOR:
_____	_____
Signature	Signature
_____	_____
Name	Name
_____	_____
Title	Title
_____	_____
Date	Date

ANNEX A: Details of Processing

Categories of Data Subjects:

- Survey respondents
- Research participants
- Consumer panel members

Categories of Personal Data:

- Demographic information (age, gender, location, income bracket)
- Survey responses and opinions
- Behavioral data (purchase history, usage patterns)
- Contact information (where provided by Client)

Sensitive Data:

The Processor does not require processing of special categories of data (Article 9 GDPR). If such data is included in Client uploads, the Client warrants it has obtained explicit consent.

Processing Operations:

- Data upload and storage
- Data transformation and cleaning
- Statistical analysis and cross-tabulation
- AI-assisted analysis and insight generation
- Report generation and export

ANNEX B: Security Measures

The technical and organizational security measures implemented by the Processor are detailed in the AIRA Analytics Data Security Policy, which is incorporated by reference and available upon request.

Summary of key measures:

- Encryption: TLS 1.3 in transit, AES-256 at rest
- Access Control: MFA, RBAC, SSO integration
- Infrastructure: SOC 2 Type II certified cloud provider
- Monitoring: 24/7 intrusion detection, audit logging
- Incident Response: 24-hour notification commitment
- Data Isolation: Logical separation per client

— End of Agreement —