Data Processing Addendum (DPA)

ProcureValue - Data Processing Addendum

This Data Processing Addendum ("**DPA**") is incorporated into the Master Services Agreement ("**MSA**") between:

1. **[Customer Legal Name]** ("**Customer**" or "**Controller**"); and
2. **Balestra Group Limited trading as ProcureValue** ("**Provider**" or "**Processor**").

This DPA applies when Provider processes Personal Data on behalf of Customer in the course of providing the Service.

1. Definitions

- Terms like "**Personal Data**," "**Data Subject**," "**Processing**," "**Controller**," and "**Processor**" have the meanings given to them in the GDPR.
- "**GDPR**" means the General Data Protection Regulation (EU) 2016/679.
- "**Service**" refers to the ProcureValue platform as defined in the MSA.

2. Roles and Scope of Processing

- **Roles.** The Parties agree that Customer is the **Controller** of Personal Data, and Provider is the **Processor**.
- **Customer's Instructions.** Provider will process Personal Data only on Customer's documented written instructions. The execution of the MSA and this DPA is Customer's primary instruction to Provider to process Personal Data to provide the Service.
- **Details of Processing.** The details of the processing (subject matter, duration, nature, purpose, etc.) are described in **Appendix 1**.
- **Provider Data.** This DPA does not apply to Provider Data, as defined in the MSA, which is independently collected by Provider and does not contain Personal Data derived from Customer Data.

3. Obligations of the Processor

Provider agrees to:

- **Security.** Implement and maintain appropriate technical and organisational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, or damage. These measures are described in **Appendix 2**.
- **Confidentiality.** Ensure that any personnel authorized to process Personal Data are bound by a strict duty of confidentiality.
- **Data Subject Rights.** To the extent legally permitted, promptly notify Customer of any request from a Data Subject to exercise their rights (e.g., access, rectification, erasure). Provider will assist Customer, at Customer's expense, with appropriate technical and organizational measures to fulfill Customer's obligation to respond to such requests.

- **Data Breach Notification.** Notify Customer **without undue delay** after becoming aware of a Personal Data Breach, providing Customer with sufficient information to meet its own notification obligations under the GDPR.

4. Sub-processing

- **General Authorization.** Customer provides Provider with a general written authorization to engage third-party sub-processors to process Personal Data, including those listed in **Appendix 3**.
- **New Sub-processors.** Provider will inform Customer (e.g., via email or an online list) of any intended changes (additions or replacements) to its sub-processors, thereby giving Customer the opportunity to object.
- **Liability.** Provider will have a written agreement with each sub-processor containing data protection obligations no less protective than those in this DPA. Provider remains fully liable to Customer for the performance of its sub-processors' obligations.

5. Audits and Compliance

Provider will make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and the GDPR. Provider will allow for and contribute to audits, including inspections, conducted by Customer or their designated auditor (at Customer's expense, during business hours, and with reasonable prior notice to avoid disruption).

6. International Data Transfers

- **Primary Processing.** Provider is based in New Zealand, a country that has received an "adequacy decision" from the European Commission. This means data transfers from the EU to New Zealand are permitted without additional safeguards.
- **Sub-processor Transfers.** For any transfers of Personal Data to sub-processors located in countries without an adequacy decision (like the United States), Provider will ensure such transfers are lawful by implementing appropriate safeguards, such as the Standard Contractual Clauses (SCCs).

7. Return or Deletion of Data

Upon termination of the MSA, Provider will delete all Personal Data processed under this DPA within 30 days, as specified in the MSA, unless EU or member state law requires its retention.

8. General

- This DPA is part of the MSA. In the event of any conflict between this DPA and the MSA regarding data processing, the terms of this DPA will prevail.

Appendix 1: Details of Processing

- **Subject Matter:** The processing of Personal Data related to the provision of the ProcureValue SaaS platform.
- **Duration:** The duration of the MSA, plus the 30-day deletion period.

- **Nature and Purpose:** To process Personal Data as necessary to provide the Service, including user account creation, survey administration, AI-driven analysis (on anonymized data), and platform support.
- **Types of Personal Data:**
    - **Account Data:** Name, email address, organization name (for registered users).
    - **Survey Invitation Data:** Business email addresses of survey respondents (processed temporarily to send invitations and deleted 90 days after campaign completion).
- **Categories of Data Subjects:**
    - **Users:** Customer's employees and contractors who are authorized to access the Service.
    - **Respondents:** Customer's employees, suppliers, or other stakeholders who are invited to take a survey.

Appendix 2: Security Measures

Provider's technical and organisational security measures are described in Provider's completed CSA Consensus Assessments Initiative Questionnaire (CAIQ), available at https://www.procurevalue.tech/en-GB/security. Provider is pursuing SOC 2 Type II certification and will update this Appendix upon completion.

Appendix 3: Sub-processors

As of the date of this DPA, Provider uses the following sub-processors:

Sub-processor	**Purpose**	**Location**
Google Cloud Platform	Cloud hosting (servers)	USA
Neon	Database hosting	USA
Neo4j	Database hosting	Singapore
MongoDB	Database hosting	USA
Cloudflare	Website hosting	Global
Resend	Transactional email delivery	USA
Tavily	Web crawling	Global
Google Gemini AI	AI analysis (of **anonymized** data)	USA