DATA PROCESSING AGREEMENT

(DPA)

This Data Processing Agreement ("DPA") is entered into as of the date last signed below (the "Effective Date"),

BETWEEN:

(1) YBSERVE SOLUTIONS (Company No: **202603018067 (NS0318440-A)**), a sole proprietorship registered in Malaysia with its principal place of business at [Insert Address] (hereinafter referred to as the **"Processor"** or **"YBServe"**);

AND

(2) [Customer Name] (Company/Entity No: [Insert]), with principal office at [Insert Address] (hereinafter referred to as the **"Controller"** or **"Customer"**).

(The Processor and Controller are hereinafter collectively referred to as the "Parties" and individually as a "Party".)

RECITALS

WHEREAS:

- The Controller is an elected representative's office, political entity, or constituency office in Malaysia that requires a digital platform for managing citizen issues, tracking resolutions, and generating reports;
- The Processor provides a multi-tenant software-as-a-service (SaaS) platform known as "YBServe" that enables digital issue management, AI-assisted classification, citizen communication, and analytics;
- In providing the Services, the Processor will process Personal Data on behalf of the Controller;
- The Parties wish to ensure that the processing of Personal Data complies with the Personal Data Protection Act 2010 (Act 709) of Malaysia ("PDPA") and its amendments;
- This DPA sets out the terms and conditions governing the processing of Personal Data by the Processor on behalf of the Controller.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the Parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

In this DPA, unless the context otherwise requires, the following terms shall have the meanings set out below:

"AI Features" means the artificial intelligence and machine learning functionalities provided as part of the Services, including but not limited to issue classification, sentiment analysis, summarisation, and automated reporting.

"AI Input" means any Personal Data, text, images, documents, or other content provided by the Controller or Data Subjects that is processed by AI Features.

"AI Output" means any classifications, predictions, summaries, suggestions, or other results generated by AI Features based on AI Input.

"Applicable Data Protection Laws" means the Personal Data Protection Act 2010 (Act 709) of Malaysia, including any amendments, subsidiary legislation, guidelines, and codes of practice issued thereunder.

"Controller" means the Party identified as such in this DPA, being the entity that determines the purposes and means of Processing Personal Data.

"Data Subject" means the identified or identifiable natural person to whom Personal Data relates, including citizens who submit issues through the Platform.

"Main Agreement" means the subscription agreement, terms of service, or other agreement between the Parties governing the provision of the Services.

"Personal Data" means any information in respect of commercial transactions, which is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose, and which relates directly or indirectly to a Data Subject, who is identified or identifiable from that information or from that and other information in the possession of the Processor, including any sensitive personal data.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

"Platform" means the YBServe software-as-a-service platform, including all features, functionalities, and related services.

"Processing" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, including collecting, recording, holding, storing, organising, adapting, altering, retrieving, consulting, using, disclosing, combining, aligning, blocking, erasing, or destroying Personal Data.

"Processor" means YBSERVE SOLUTIONS, the Party identified as such in this DPA, being the entity that Processes Personal Data on behalf of the Controller.

"Security Measures" means the technical and organisational measures described in Annex B to protect Personal Data against unauthorised or unlawful Processing, accidental loss, destruction, or damage.

"Services" means the services provided by the Processor to the Controller under the Main Agreement, including access to and use of the Platform.

"Sub-processor" means any third party appointed by or on behalf of the Processor to Process Personal Data on behalf of the Controller in connection with this DPA.

1.2 Interpretation

In this DPA, unless the context otherwise requires: (a) references to clauses, annexes, and schedules are to clauses of, and annexes and schedules to, this DPA; (b) headings are for convenience only and shall not affect interpretation; (c) words in the singular include the plural and vice versa; (d) references to any legislation include amendments and re-enactments thereof; and (e) where there is any conflict between the Main Agreement and this DPA regarding data protection matters, this DPA shall prevail.

2. SCOPE AND PURPOSE OF PROCESSING

2.1 Scope

This DPA applies to all Processing of Personal Data by the Processor on behalf of the Controller in connection with the Services.

2.2 Purpose

The Processor shall Process Personal Data only for the following purposes:

- Receiving and storing citizen issue submissions;
- AI-assisted classification, categorisation, and prioritisation of issues;
- Generating analytics, reports, and insights for the Controller;
- Facilitating communication between the Controller and Data Subjects;
- Maintaining audit trails and records as required by law;
- Any other purpose as documented in Annex A or as instructed by the Controller in writing.

2.3 Categories of Data Subjects

The categories of Data Subjects whose Personal Data may be Processed include:

- Citizens and constituents who submit issues through the Platform;
- Authorised users of the Platform (staff, volunteers, administrators);
- Third parties mentioned in issue submissions.

2.4 Types of Personal Data

The types of Personal Data Processed may include, but are not limited to, those specified in Annex A.

3. ROLES AND RESPONSIBILITIES

3.1 Controller Responsibilities

The Controller shall:

- Determine the purposes and means of Processing Personal Data;
- Ensure that it has a lawful basis for Processing Personal Data, including obtaining valid consent from Data Subjects where required;
- Provide clear and accurate privacy notices to Data Subjects;
- Respond to requests from Data Subjects exercising their rights under Applicable Data Protection Laws;
- Ensure that instructions given to the Processor comply with Applicable Data Protection Laws;
- Notify the Processor promptly of any changes to data protection requirements that may affect the Services.

3.2 Processor Responsibilities

The Processor shall:

- Process Personal Data only in accordance with documented instructions from the Controller, unless required to do so by Malaysian law;
- Ensure that persons authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Implement and maintain the Security Measures described in Annex B;
- Assist the Controller in ensuring compliance with its obligations under Applicable Data Protection Laws;
- Not Process Personal Data for any purpose other than as specified in this DPA or as instructed by the Controller;
- Promptly inform the Controller if, in the Processor's opinion, an instruction from the Controller infringes Applicable Data Protection Laws.

4. SUB-PROCESSING

4.1 Authorised Sub-processors

The Controller provides general authorisation for the Processor to engage the Sub-processors listed in Annex C. The Processor shall ensure that any Sub-processor is bound by data protection obligations no less protective than those in this DPA.

4.2 Changes to Sub-processors

The Processor shall notify the Controller of any intended changes concerning the addition or replacement of Sub-processors at least fourteen (14) days in advance. The Controller may object to such changes on reasonable grounds within seven (7) days of notification. If the Parties cannot resolve the objection, the Controller may terminate the affected Services.

4.3 Liability for Sub-processors

The Processor shall remain fully liable to the Controller for the performance of its Sub-processors' obligations under this DPA.

5. SECURITY MEASURES

5.1 Implementation

The Processor shall implement and maintain the technical and organisational measures described in Annex B to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration, or disclosure.

5.2 Assessment

The Processor shall regularly assess the effectiveness of Security Measures and make improvements as necessary to address evolving threats and vulnerabilities.

5.3 Personnel

The Processor shall ensure that its personnel who have access to Personal Data are trained in data protection requirements and are bound by appropriate confidentiality obligations.

6. PERSONAL DATA BREACH

6.1 Notification

The Processor shall notify the Controller without undue delay, and in any event within forty-eight (48) hours, upon becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of the Controller.

6.2 Information

Such notification shall include, to the extent known:

- A description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records affected;
- The name and contact details of the Processor's data protection contact;

- The likely consequences of the Personal Data Breach;
- The measures taken or proposed to be taken to address the Personal Data Breach and mitigate its effects.

6.3 Cooperation

The Processor shall cooperate with the Controller and take such reasonable steps as are directed by the Controller to assist in the investigation, mitigation, and remediation of the Personal Data Breach.

6.4 Controller Notification Obligations

The Controller retains responsibility for determining whether to notify the Personal Data Protection Commissioner and affected Data Subjects in accordance with Applicable Data Protection Laws.

7. DATA SUBJECT RIGHTS

7.1 Assistance

The Processor shall assist the Controller in responding to requests from Data Subjects exercising their rights under Applicable Data Protection Laws, including rights of access, correction, withdrawal of consent, restriction of processing, and prevention of processing likely to cause damage or distress.

7.2 Notification

If the Processor receives a request from a Data Subject relating to Personal Data Processed on behalf of the Controller, the Processor shall promptly forward such request to the Controller and shall not respond directly unless instructed to do so by the Controller.

7.3 Time Limits

The Processor shall provide reasonable assistance to enable the Controller to respond to Data Subject requests within the time limits prescribed by Applicable Data Protection Laws.

8. ARTIFICIAL INTELLIGENCE PROCESSING

8.1 Scope of AI Processing

The Services include AI Features that Process Personal Data for classification, categorisation, sentiment analysis, summarisation, and reporting purposes. The Controller acknowledges and consents to such AI Processing as described in this DPA and Annex A.

8.2 Third-Party AI Providers

The Processor engages third-party AI service providers (as listed in Annex C) to deliver AI Features. Such providers are bound by data processing agreements requiring them to:

- Process AI Input only as necessary to provide the AI functionality;
- Not use AI Input to train, improve, or develop their general AI models;
- Delete AI Input after Processing is complete in accordance with their retention policies;
- Implement appropriate security measures to protect AI Input and AI Output.

8.3 AI Output

AI Output is advisory only and does not constitute a decision by the Processor. The Controller retains full discretion over all decisions regarding the handling of citizen issues.

8.4 Data Minimisation

The Processor shall ensure that only Personal Data necessary for the specific AI function is transmitted to third-party AI providers.

9. CROSS-BORDER DATA TRANSFERS

9.1 General Prohibition

The Processor shall not transfer Personal Data outside Malaysia except where:

- The Controller has provided documented instructions authorising such transfer;
- The transfer is to a place specified by the Minister as having adequate protection for Personal Data;
- The Data Subject has consented to the transfer; or
- The transfer is necessary for the performance of the Services and appropriate safeguards are in place.

9.2 Sub-processor Locations

The locations of Sub-processors are specified in Annex C. The Controller acknowledges that certain Sub-processors may Process Personal Data outside Malaysia and consents to such transfers subject to the safeguards described therein.

10. AUDIT AND INSPECTION

10.1 Audit Rights

The Controller may, upon reasonable notice and during normal business hours, request information and documentation demonstrating the Processor's compliance with this DPA. Such requests shall not occur more than once per calendar year unless a Personal Data Breach has occurred.

10.2 Cooperation

The Processor shall provide reasonable cooperation and access to relevant information, systems, and personnel to enable the Controller to verify compliance with this DPA.

10.3 Third-Party Audits

Upon request, the Processor shall provide the Controller with copies of relevant third-party certifications, audit reports, or security assessments.

11. DATA RETENTION AND DELETION

11.1 Retention Period

The Processor shall retain Personal Data only for as long as necessary to perform the Services or as required by Applicable Data Protection Laws, whichever is longer.

11.2 Deletion Upon Termination

Upon termination or expiry of the Main Agreement, or upon the Controller's written request, the Processor shall:

- Return to the Controller, in a commonly used format, all Personal Data in the Processor's possession; and/or
- Securely delete or anonymise all Personal Data within thirty (30) days, except to the extent that retention is required by law.

11.3 Certification

Upon request, the Processor shall provide written certification that Personal Data has been deleted in accordance with this Clause.

12. CONFIDENTIALITY

The Processor shall maintain the confidentiality of all Personal Data and shall not disclose Personal Data to any third party except as authorised by this DPA, instructed by the Controller, or required by law. This obligation shall survive the termination of this DPA.

13. LIABILITY AND INDEMNIFICATION

13.1 Liability

Each Party shall be liable for damages arising from its breach of this DPA or Applicable Data Protection Laws. The liability of the Processor shall be subject to any limitations set forth in the

Main Agreement, except that such limitations shall not apply to liability arising from the Processor's gross negligence, wilful misconduct, or breach of its confidentiality obligations.

13.2 Indemnification

The Processor shall indemnify and hold harmless the Controller against all claims, liabilities, damages, and expenses (including reasonable legal fees) arising from the Processor's breach of this DPA, subject to the limitations in the Main Agreement.

14. TERM AND TERMINATION

14.1 Term

This DPA shall come into effect on the Effective Date and shall remain in force for as long as the Processor Processes Personal Data on behalf of the Controller.

14.2 Survival

The provisions of this DPA that by their nature should survive termination (including Clauses 6, 11, 12, and 13) shall survive the termination or expiry of this DPA.

15. GENERAL PROVISIONS

15.1 Governing Law

This DPA shall be governed by and construed in accordance with the laws of Malaysia. Any disputes arising under or in connection with this DPA shall be subject to the exclusive jurisdiction of the courts of Malaysia.

15.2 Amendments

This DPA may only be amended by a written instrument signed by authorised representatives of both Parties.

15.3 Severability

If any provision of this DPA is held to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect.

15.4 Entire Agreement

This DPA, together with the Main Agreement and its Annexes, constitutes the entire agreement between the Parties with respect to the Processing of Personal Data and supersedes all prior agreements, representations, and understandings relating thereto.

15.5 Notices

All notices under this DPA shall be in writing and shall be deemed given when delivered personally, sent by email with confirmation of receipt, or sent by registered mail to the addresses specified in the Main Agreement.

IN WITNESS WHEREOF

The Parties have executed this Data Processing Agreement as of the Effective Date.

For and on behalf of **YBSERVE SOLUTIONS** (Processor) ________________________________ Signature Name: __________________________ Title: __________________________ Date: __________________________	**For and on behalf of** **[CONTROLLER NAME]** (Controller) ________________________________ Signature Name: __________________________ Title: __________________________ Date: __________________________

ANNEX A: DATA PROCESSING DETAILS

A.1 Categories of Data Subjects

- Citizens and constituents of the Controller's constituency
- Staff and volunteers of the Controller authorised to use the Platform
- Third parties referenced in citizen submissions

A.2 Types of Personal Data

Citizen Data:

- Full name
- Email address
- Phone number
- Partial MyKad number (last 4 digits)
- Address (optional)
- Geographic identifiers (PDM, DUN, Parliamentary constituency)
- Demographic information (age, gender, occupation, race, religion - if provided)
- Issue descriptions and attachments (which may contain additional Personal Data)

Staff/User Data:

- Full name
- Email address
- Role within the organisation
- Activity logs and audit trails

A.3 Processing Activities

Activity	Description
Issue Intake	Collection and storage of citizen-submitted issues via public web forms
AI Classification	Automated categorisation, prioritisation, and sentiment analysis of issues using AI
Communication	Sending email notifications to citizens regarding issue status updates
Analytics	Generating aggregated reports, dashboards, and constituency insights
Audit Logging	Recording all actions taken on issues for accountability and compliance

ANNEX B: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

B.1 Access Control

- Role-based access control (RBAC) with defined roles: Admin, Staff, Volunteer
- Multi-tenant architecture with strict data isolation using Row Level Security (RLS)
- Secure authentication using industry-standard protocols
- Password policies enforcing minimum complexity requirements
- Session management with automatic timeout

B.2 Data Encryption

- All data encrypted in transit using TLS 1.2 or higher
- All data encrypted at rest using AES-256 encryption
- Database connections secured with SSL/TLS
- Secure key management practices

B.3 Network Security

- Web Application Firewall (WAF) protection
- DDoS mitigation and protection
- Rate limiting on all API endpoints
- HTTPS enforced on all connections

B.4 Infrastructure Security

- Hosting on SOC 2 compliant cloud infrastructure
- Automatic failover and redundancy
- Regular security patches and updates
- Automated backups with point-in-time recovery

B.5 Monitoring and Logging

- Comprehensive audit logging of all data access and modifications
- Real-time monitoring for security anomalies
- Log retention in accordance with legal requirements
- Incident alerting and response procedures

B.6 Personnel Security

- Background checks for personnel with access to Personal Data
- Confidentiality agreements for all personnel
- Regular security awareness training
- Principle of least privilege for data access

B.7 Business Continuity

- Disaster recovery procedures with defined recovery time objectives
- Regular backup testing and verification
- Geographic redundancy for critical systems

ANNEX C: APPROVED SUB-PROCESSORS

The following Sub-processors are authorised to Process Personal Data on behalf of the Controller as of the Effective Date:

Sub-processor	Purpose	Location	Data Processed
Supabase Inc.	Database hosting, authentication, and file storage	Singapore (ap-southeast-1)	All Personal Data
Vercel Inc.	Application hosting and serverless functions	Global (Edge network)	Request/session data
OpenAI, LLC	AI classification for text-only issues	United States	Issue text content
Anthropic PBC	AI classification for issues with images	United States	Issue text and images
Resend Inc.	Transactional email delivery	United States	Email addresses, names
Stripe Inc.	Payment processing and subscription management	Global	Billing information

Note: This list may be updated in accordance with Clause 4.2 of this DPA. The Controller will be notified of any changes.

— END OF AGREEMENT —