

DATA PROCESSING AGREEMENT

(DPA)

Version 3.0 | Confidential

Personal Data Protection Act 2010 (Act 709)

as amended by the Amendment Act 2024 (Act A1727)

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 Executive Suite 2, Level 3, Wisma Suria, Jalan Teknokrat 6, Cyber 5, 63000 Cyberjaya, Selangor, Malaysia (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").

RECITALS

- The Controller is an elected representative's office, political entity, or constituency office in Malaysia;
- The Processor provides a multi-tenant SaaS platform known as "YBServe";
- In providing the Services, the Processor will process Personal Data on behalf of the Controller;
- The Parties wish to ensure compliance with the **PDPA 2010 as amended by the Amendment Act 2024**;
- This DPA sets out the terms governing the processing of Personal Data.

1. DEFINITIONS AND INTERPRETATION

"Applicable Data Protection Laws" means the PDPA 2010 (Act 709), the Amendment Act 2024 (Act A1727), and all subsidiary legislation, guidelines, and codes of practice.

"Biometric Data" means personal data resulting from technical processing relating to physical, physiological, or behavioural characteristics, as defined by the Amendment Act 2024.

"Controller" means the Customer who determines the purposes and means of Processing Personal Data.

"Data Protection Officer" means the person appointed under Section 12 of the PDPA (as amended) to monitor compliance.

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

"Processor" means YBSERVE SOLUTIONS.

"Sensitive Personal Data" includes physical/mental health, political opinions, religious beliefs, **Biometric Data**, commission of offences.

"Transfer Impact Assessment" means an assessment of destination country data protection laws per the Cross-Border Personal Data Transfer Guidelines.

2. SCOPE AND PURPOSE OF PROCESSING

The Processor shall Process Personal Data only for: receiving citizen interaction submissions; voter verification; AI-assisted classification and sentiment analysis; generating analytics and reports; facilitating communication; maintaining audit trails; and any other purpose documented in Annex A.

3. ROLES AND RESPONSIBILITIES

3.1 Controller Responsibilities

- Determine purposes and means of Processing;
- Obtain valid consent from Data Subjects;
- Respond to Data Subject requests (access, correction, data portability);
- Assess whether DPO appointment is required;
- Determine whether to notify Commissioner following a breach.

3.2 Processor Responsibilities

- Process Personal Data only per documented instructions;
- **Comply directly with the Security Principle under Section 9 of the PDPA (Amendment Act 2024);**
- Implement and maintain Security Measures (Annex B);
- **Provide sufficient guarantees of technical and organisational security measures.**

4. SUB-PROCESSING

The Controller provides general authorisation for Sub-processors listed in Annex C. The Processor shall notify of changes 14 days in advance. The Processor remains fully liable for Sub-processors.

5. SECURITY MEASURES

The Processor shall implement and maintain measures in Annex B, regularly assess their effectiveness, and ensure personnel are trained and bound by confidentiality.

6. PERSONAL DATA BREACH

6.1 Notification

The Processor shall notify the Controller without undue delay, and within **seventy-two (72) hours**, upon becoming aware of a Personal Data Breach.

6.2 Information

Notification shall include: nature of breach, categories and numbers affected, likely consequences, and measures taken.

6.3 Controller Notification Obligations

Under **Section 12B of the PDPA** (Amendment Act 2024), the Controller must notify the Commissioner **within 72 hours** and affected Data Subjects **without unnecessary delay** where significant harm is likely. The Processor shall assist.

7. DATA SUBJECT RIGHTS

The Processor shall assist the Controller in responding to Data Subject requests including access, correction, withdrawal of consent, and **data portability under Section 43A of the PDPA** (Amendment Act 2024). Data shall be provided in CSV or JSON format upon request.

8. ARTIFICIAL INTELLIGENCE PROCESSING

AI Features process data for classification, sentiment analysis, summarisation, and chatbot intake. Third-party AI providers (Annex C) are bound not to train on Customer data. AI Output is advisory only.

Data Minimisation: The Processor shall, where technically feasible, strip personally identifying information (names, IC numbers, phone numbers, email addresses) from AI Input before transmission to third-party providers.

9. CROSS-BORDER DATA TRANSFERS

9.1 Legal Framework

Transfers are permissible under **Section 129 of the PDPA** (as amended) where: (a) substantially similar law or adequate protection exists; (b) Data Subject consent; (c) contractual necessity; (d) legal proceedings; (e) reasonable precautions; or (f) vital interests.

9.2 Record-Keeping

The Processor maintains records of all cross-border transfers including receiver details, destination, data types, purposes, legal basis, and evidence of compliance.

9.3 Transfer Impact Assessment

TIAs have been conducted for each destination country in Annex C per the CBPDT Guidelines (29 April 2025). TIAs are valid for 3 years and available to the Controller upon request.

10. DATA PROTECTION OFFICER

The Processor has designated a data protection contact: privacy@ybserve.com. The Controller shall assess whether DPO appointment is required under Section 12 of the PDPA (as amended).

11. AUDIT, RETENTION, CONFIDENTIALITY, LIABILITY

The Controller has annual audit rights. Personal Data is retained only as necessary and deleted within 30 days of termination. The Processor maintains confidentiality. Each Party is liable for its breach of this DPA. These and surviving clauses continue after termination.

12. GENERAL PROVISIONS

Governed by Malaysian law. Amendments require written agreement. This DPA prevails over the Main Agreement on data protection matters.

IN WITNESS WHEREOF

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

Citizen Data: Full name, email, phone, **full MyKad (IC) number**, address (optional), geographic identifiers (PDM/DUN/Parliament), demographic info (if provided), interaction descriptions and attachments, photos, chat messages, sentiment data (AI-generated), tracking codes.

Staff/User Data: Full name, email, role, login credentials (hashed), activity logs, consent records.

Processing Activities:

Activity	Description
Interaction Intake	Collection via public web forms and chat
Voter Verification	IC number verification against electoral roll
AI Classification	Categorisation, prioritisation, sentiment analysis
Communication	Email notifications and real-time chat
Analytics	Reports, dashboards, constituency insights
Audit Logging	All actions logged for accountability

ANNEX B: SECURITY MEASURES

Access Control:

- RBAC (Admin, Staff, Volunteer)
- Row Level Security (RLS) for tenant isolation
- bcrypt password hashing
- Secure httpOnly session tokens

Encryption:

- TLS 1.2+ in transit
- AES-256 at rest
- SSL/TLS database connections

Network:

- DDoS protection
- Rate limiting (5/phone/email/IC/day, 500/tenant/day)
- HTTPS enforced

Infrastructure:

- SOC 2 compliant cloud (Supabase/AWS)
- Automated backups with PITR
- Serverless co-located in Singapore (Vercel sin1)

Monitoring:

- Audit logging of all data access
- Sentry error monitoring with PII stripped before transmission
- No Personal Data stored in error monitoring

AI Data Minimisation:

- PII stripped before AI transmission where feasible
- AI providers receive minimum necessary data

ANNEX C: APPROVED SUB-PROCESSORS

Sub-processor	Purpose	Location	Data	Legal Basis
Supabase Inc.	Database, auth, storage	Singapore (AWS ap-se-1)	All Personal Data	S.129(2)(a) Similar law + S.129(3)(a) Consent. TIA conducted.
Vercel Inc.	Hosting, serverless	Singapore (sin1)	Request data (no PD at rest)	S.129(2)(a) Compute only
OpenAI, LLC	AI text classification	United States	Text content (PII minimised)	S.129(3)(a) Consent + S.129(3)(f) Precautions
Anthropic PBC	AI text + image class.	United States	Text + images (PII minimised)	S.129(3)(a) Consent + S.129(3)(f) Precautions
Resend Inc.	Email delivery	United States	Email, names	S.129(3)(f) Precautions
Stripe Inc.	Payments	Global	Billing only (no citizen PD)	S.129(3)(b) Contract
Sentry	Error monitoring	United States	Error logs (PII stripped)	No PD transferred

Note: This list may be updated per Clause 4. Controller notified 14 days in advance.

-- END OF AGREEMENT --