Data Processing Agreement

Effective date: 12 July 2026

This Data Processing Agreement (?DPA?) forms part of the Terms of Service between [Operator Legal Name] (?Processor?, ?we?) and the customer (?Controller?, ?you?) and governs the Processing of Personal Data by us on your behalf when you use Impact365 (the ?Service?). Capitalised terms follow the meanings in the Malaysian Personal Data Protection Act 2010 (?PDPA?).

1. Roles of the parties

For Personal Data that you (or your users) upload about your own clients, employees, directors and shareholders, you act as the data user/Controller and we act as the data processor/Processor, Processing such Personal Data only on your documented instructions (including via your use of the Service).

2. Subject matter, nature & duration

- ? Subject matter: provision of the Service as described in the Terms.
- ? Nature & purpose: hosting, storage, organisation, retrieval, transmission and deletion of Customer Data to operate accounting, company-secretarial, HR/payroll, document and AI features.
- ? Duration: the term of your subscription plus any retention period required by law.

3. Categories of data & data subjects

- ? Data subjects: your authorised users, customers/suppliers, employees, directors, shareholders.
- ? Personal Data: names, contact details, identification numbers (NRIC/passport), addresses, financial and transactional records, employment and payroll data, and uploaded documents.

4. Our obligations as Processor

- ? Process Personal Data only on your documented instructions, unless required by law.
- ? Ensure personnel authorised to Process Personal Data are bound by confidentiality.
- ? Implement appropriate technical and organisational security measures (clause 6).
- ? Assist you, taking into account the nature of Processing, in responding to data-subject requests and in meeting your security, breach-notification and (where applicable) impact-assessment obligations.
- ? At your choice, delete or return Customer Data at the end of the engagement, subject to legal retention.
- ? Make available information reasonably necessary to demonstrate compliance with this DPA.

5. Sub-processing

You provide general authorisation for us to engage sub-processors to support the Service. We impose data-protection obligations on each sub-processor that are no less protective than this DPA, and we remain responsible for their performance. We will give reasonable notice of any

intended addition or replacement of a sub-processor so you may object on reasonable grounds.

Current sub-processors

Sub-processor	Purpose	Location
[Cloud Hosting Provider]	Application & database hosting, storage	[Region]
GajiHub	HR & payroll data integration (when enabled by you)	Malaysia
[AI Provider ? e.g. Anthropic / OpenAI]	AI assistant features (when enabled)	[Region]
[Email Provider]	Transactional email & notifications	[Region]

This list is a template. Maintain an accurate, up-to-date sub-processor list reflecting your actual vendors.

6. Security measures

- Strict logical tenant isolation between customers.
- One-way hashing of passwords and API tokens; access on a need-to-know basis.
- Role-based access control and audit logging of sensitive actions.
- Encryption of data in transit; environment hardening and monitoring.
- Backup and recovery procedures.

7. Data-subject requests

Where we receive a request directly from a data subject relating to your Customer Data, we will, where lawful, refer the request to you and assist you in responding.

8. Personal Data breach

We will notify you without undue delay after becoming aware of a Personal Data breach affecting your Customer Data, and provide information reasonably available to help you meet your obligations.

9. International transfers

Where Processing occurs outside Malaysia (including by sub-processors), we take steps to ensure a level of protection consistent with the PDPA.

10. Audit

On reasonable prior written notice and subject to confidentiality, we will make available information necessary to demonstrate compliance and allow for reasonable audits, no more than once per year except where required by a regulator.

11. Return & deletion

On termination, you may export Customer Data for a limited period, after which we will delete or anonymise it in the ordinary course, save where retention is required by law.

12. Contact

Data protection contact: support@slv.my.