This Data Processing Addendum (this "Addendum") forms part of the Master Services Agreement (the "Agreement") between Growth Fuel Consulting Pte. Ltd. (UEN 202307909D) (the "Company") and the Client, and governs the processing by the Company of personal data on the Client's behalf in the course of providing the Services. Capitalised terms not defined in this Addendum have the meanings given in the Agreement.

1. DEFINITIONS

1.1 **"Applicable Data Protection Law"** means the Personal Data Protection Act 2012 of Singapore (the "PDPA"), together with any other data protection law identified by the Client in writing and agreed by the Parties in a Service Order in accordance with clause 2.4.

1.2 **"Client Personal Data"** means personal data that the Company processes on the Client's behalf in the course of providing the Services.

1.3 **"data intermediary"**, **"individual"**, **"personal data"** and **"processing"** have the meanings given to them in the PDPA.

1.4 **"Sub-processor"** means any third party engaged by the Company to process Client Personal Data.

1.5 A reference to a clause or Schedule is a reference to a clause of, or Schedule to, this Addendum unless stated otherwise. The Schedules form part of this Addendum.

2. ROLES OF THE PARTIES

2.1 The Client is the organisation responsible for Client Personal Data and determines the purposes for which it is processed. The Company processes Client Personal Data solely as a data intermediary on the Client's behalf.

2.2 Where the Client itself processes Client Personal Data as a data intermediary or equivalent for a third party, the Company acts as a further intermediary on the Client's behalf, and the Client warrants that its arrangements with that third party permit the Company's engagement on the terms of this Addendum.

2.3 This Addendum does not apply to personal data for which the Company is the organisation responsible in its own right, including the business contact information of the Client's personnel used to administer the relationship. That data is handled in accordance with the Company's Privacy Notice.

2.4 The obligations of the Company under this Addendum are framed by reference to the PDPA. The Company assumes no obligation under the data protection law of any other jurisdiction, including the General Data Protection Regulation (EU) 2016/679, the law of the United Kingdom or the Privacy Act 1988 of Australia, unless that law and any additional terms, including any required transfer mechanism, are identified in writing and agreed by the Parties in the relevant Service Order.

3. SCOPE AND INSTRUCTIONS

3.1 The Company processes Client Personal Data only on the documented instructions of the Client, including as set out in this Addendum, the Agreement and each Service Order, and as necessary to provide the Services. The Client's configuration of the systems that the Company manages, together with the Agreement and each Service Order, constitutes the Client's complete instructions.

3.2 The Company will inform the Client if, in its opinion, an instruction infringes Applicable Data Protection Law, though the Company is not obliged or qualified to provide legal advice.

3.3 The Company will not use Client Personal Data for its own purposes. The Company's right under the clause of the Agreement headed Transfer of Property and Intellectual Property Rights to use data generated through the performance of the Services extends only to data that is aggregated and anonymised so that neither the Client nor any individual is identifiable from it, and confers no right over Client Personal Data.

3.4 The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of individuals are set out in Schedule 1.

3.5 The Client is responsible for the lawfulness of any identifier, data field or authentication method that it instructs the Company to implement or maintain in its systems, including any use of national identification numbers such as NRIC, FIN or passport numbers. The Client warrants that such instructions comply with Applicable Data Protection Law, including any applicable advisory guidelines of the Personal Data Protection Commission. The Company may raise concerns regarding such an instruction without assuming responsibility for the Client's compliance.

4. SUB-PROCESSORS

4.1 The Client grants the Company general authorisation to engage Sub-processors to process Client Personal Data. The Sub-processors engaged as at the date of this Addendum, and the locations in which they hold data, are listed in Schedule 2.

4.2 The Company will impose on each Sub-processor data protection obligations no less protective than those in this Addendum, and remains liable to the Client for each Sub-processor's performance.

4.3 The Company will give the Client at least thirty (30) days' written notice of any intended addition or replacement of a Sub-processor. During that period the Client may object on reasonable data protection grounds. The Parties will work in good faith to resolve any objection. Where it cannot be resolved, the Client may terminate the affected Services on reasonable written notice.

5. SECURITY

5.1 The Company will implement and maintain technical and organisational measures to protect Client Personal Data against unauthorised or unlawful processing and against accidental loss,

destruction, damage, alteration or disclosure, appropriate to the harm that might result and to the nature of the data.

5.2 The measures implemented by the Company are set out in Schedule 3. The Company may update those measures from time to time, provided that no update materially reduces the overall level of protection.

5.3 The Company will ensure that personnel authorised to process Client Personal Data are bound by appropriate confidentiality obligations.

5.4 The Client shall not transmit any password, access credential or authentication secret to the Company by unencrypted email, chat or other insecure means. The Company will provide a secure method for sharing credentials where a credential must be shared. Wherever a platform supports it, the Parties will use delegated or named-user access in preference to shared credentials.

6. PERSONNEL AND LOCATION

6.1 The Company engages personnel located in Singapore and in Malaysia. Personnel in Malaysia are engaged through an employer of record and may access Client Personal Data in the course of providing the Services.

6.2 The Company ensures that all personnel, wherever located, and the employer of record engaging them, are bound by written obligations providing a standard of protection for Client Personal Data comparable to that required under the PDPA, including obligations of confidentiality.

7. CROSS-BORDER TRANSFERS

7.1 Where the Company transfers Client Personal Data outside Singapore, including to the Sub-processors listed in Schedule 2 and to its personnel in Malaysia, the Company will satisfy itself that the recipient is bound by legally enforceable obligations to provide the transferred data a standard of protection comparable to that under the PDPA, in accordance with section 26 of the PDPA.

7.2 Where a data protection regime other than the PDPA has been agreed in a Service Order under clause 2.4, any transfer mechanism required by that regime shall be as set out in that Service Order.

8. ASSISTANCE TO THE CLIENT

8.1 Taking into account the nature of the processing, the Company will provide reasonable assistance to the Client, by appropriate technical and organisational measures, in responding to requests from individuals exercising rights under Applicable Data Protection Law, including requests for access to or correction of Client Personal Data.

8.2 Where the Company receives a request directly from an individual in respect of Client Personal Data, it will not respond to the request itself, other than to direct the individual to the Client, and will promptly notify the Client.

8.3 The Company will provide the Client with reasonable assistance in relation to any assessment, notification or consultation that the Client is required to make under Applicable Data Protection Law, to the extent it relates to the Company's processing.

9. DATA BREACHES

9.1 The Company will notify the Client without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a data breach affecting Client Personal Data. For this purpose the Company becomes "aware" of a breach when it has a reasonable degree of certainty that a breach affecting Client Personal Data has occurred. Where a breach originates with a Sub-processor, the Company's obligation runs from the time that Sub-processor notifies the Company of the breach.

9.2 The notification will describe, to the extent then known, the nature of the breach, the categories and approximate number of individuals and records affected, the likely consequences, and the measures taken or proposed. Where the information is not all available at once, it may be provided in phases without undue further delay.

9.3 The Company will cooperate with the Client and take reasonable steps to assist in the investigation, mitigation and remediation of any such breach.

9.4 Notification of, or assistance in relation to, a breach under this clause is not an acknowledgement by the Company of any fault or liability.

9.5 The Client remains responsible for its own obligations under Applicable Data Protection Law in respect of a breach, including any assessment of notifiability and any notification to the Personal Data Protection Commission or affected individuals.

10. CHILDREN'S AND OTHER SENSITIVE DATA

10.1 Where the Services involve Client Personal Data relating to children or other data of a sensitive nature, the Company will process it strictly in accordance with the Client's instructions and will not determine any purpose for it. In doing so the Company will have regard to the Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment issued by the Personal Data Protection Commission, to the extent they apply to a data intermediary.

10.2 Any additional requirements applicable to such data, including requirements arising from the Client's own regulatory obligations, shall be set out in the relevant Service Order.

11. AUDIT

11.1 The Company will make available to the Client information reasonably necessary to demonstrate compliance with this Addendum, and will allow for and contribute to audits conducted by the Client or an auditor mandated by it. Audits are subject to reasonable advance

notice, confidentiality obligations, and a frequency of no more than once in any twelve-month period unless required by a supervisory authority or following a breach affecting Client Personal Data.

12. RETURN AND DELETION

12.1 On termination or expiry of the Services, the Company will, at the Client's choice, return or delete Client Personal Data, and delete existing copies, except to the extent that retention is required by law. Where the Client makes no election within thirty (30) days of termination, the Company may delete.

12.2 As part of this process the Company will relinquish administrative and other access to the Client's systems in accordance with the clause of the Agreement headed Term and Termination.

13. PRECEDENCE, LIABILITY AND GENERAL

13.1 This Addendum forms part of the Agreement. In the event of conflict on the subject of data protection between this Addendum, the Agreement and any Service Order, this Addendum prevails.

13.2 The liability of each Party under or in connection with this Addendum is subject to the limitations and exclusions set out in the clause of the Agreement headed Limitations on Damages, which apply to this Addendum as they apply to the Agreement.

13.3 This Addendum is governed by the law stated in the Agreement and is subject to the same dispute resolution provisions.

SCHEDULE 1 — DETAILS OF PROCESSING

Subject matter	**Provision of configuration, implementation, integration and managed services for the Client's business platforms**
Duration	The Term of the Agreement and any Service Order
Nature and purpose	Configuring, migrating, integrating, operating and supporting the Client's systems as instructed
Types of personal data	To be completed per engagement. Typically: names, business contact details, and any personal data held within the Client's CRM, project, telephony or application systems. Identification numbers, including NRIC, FIN or passport numbers, may fall within scope for some engagements where held in the Client's systems; clause 3.5 applies to any instruction concerning their use
Categories of individuals	To be completed per engagement. Typically: the Client's own customers, prospects, employees and contacts

Special or children's data	State whether the engagement involves any. Complete for education-sector clients

SCHEDULE 2 — SUB-PROCESSORS

The Sub-processors engaged in respect of a particular Client may be narrower than this list, depending on the platforms within scope of the relevant Service Order.

Sub-processor	Purpose	Data hosting location
HubSpot, Inc.	CRM, marketing and website platform	United States
Google LLC	Email, storage, collaboration, meetings and recordings	United States
Asana, Inc.	Project and task management	United States (EU data residency available)
Slack Technologies / Salesforce, Inc.	Internal messaging	United States
Zapier, Inc.	Workflow automation	United States
Aircall SAS	Telephony and call recording	Call recordings: Sydney, Australia. Other data: United States
Softr GmbH	Application platform	European Union
PandaDoc, Inc.	Electronic signature	United States
Cloudflare, Inc.	Secure web gateway / Zero Trust network (inspects some traffic)	Global edge network
Anthropic, PBC	AI assistant (Claude) used in service delivery and internal work	United States

A written data processing agreement is in force with each Sub-processor. Cloudflare is included because TLS inspection is enabled on part of the Company's network traffic, which may include Client Personal Data in transit.

SCHEDULE 3 — TECHNICAL AND ORGANISATIONAL MEASURES

1. Governance. Information security and data protection are governed by a documented policy framework aligned to ISO/IEC 27001 (to which the Company does not claim certification). A Data Protection Officer is appointed and identified in the Company's Privacy Notice. Policies are reviewed at least annually.

2. Identity and access management. Identity, access and device management are operated through JumpCloud. Access to Client Personal Data is granted on a least-privilege basis and limited to personnel engaged on the relevant matter. Multi-factor authentication is enforced. User access is reviewed at least annually, and access within the primary identity platform is

reviewed every ninety (90) days. Access is revoked no later than the individual's final day of engagement. Dormant and inactive accounts are investigated and actioned.

3. Client system access. Wherever a platform supports it, access to Client systems is obtained through delegated or named-user access rather than shared credentials. HubSpot access is granted by the Client through partner access; no Client credential is created, transmitted or stored. Where a credential must be held, it is generated and stored in an enterprise password manager and is not stored in documents, messages, spreadsheets or code. Where the Company holds partner access to a Client HubSpot portal, that access is automatically removed after ninety (90) days of inactivity.

4. Device and endpoint security. Devices used to access Client Personal Data are centrally managed. Full-disk encryption is enforced on all managed devices. Endpoint protection against malware is deployed on all managed devices. Operating system patches are applied through managed patching with no deferral period.

5. Network security. The Company operates a Zero Trust secure web gateway (Cloudflare) for access to its systems, with TLS inspection and data loss prevention controls applied to part of its traffic.

6. Encryption in transit and at rest. Access to the platforms holding Client Personal Data is over TLS. Each platform encrypts data at rest in accordance with its published standards. Data held locally on a managed device is protected by full-disk encryption.

7. Personnel. All personnel, wherever located, are bound by written confidentiality and data protection obligations providing a standard of protection comparable to that required under the PDPA. Personnel are required to complete security awareness training at least annually.

8. Incident response. Suspected and confirmed incidents are handled under the Company's documented incident policy, including assessment of the nature and extent of the incident, the personal data affected and the likelihood of harm. Client notification is governed by clause 9 of this Addendum.

9. Continuity and recovery. Client-related data held by the Company resides in established cloud platforms providing infrastructure-level resilience. Deleted HubSpot records are recoverable for ninety (90) days, and weekly HubSpot backups are maintained in addition to platform-native recovery.

10. Return and deletion. On termination, Client Personal Data is returned or deleted at the Client's choice in accordance with clause 12, and administrative access to Client systems is relinquished.