Data Processing Addendum

This Data Processing Addendum (“Addendum“) forms part of the BGL Cloud Software Subscription Agreement (“Principal Agreement“).

WHEREAS

A. You act as a Data Controller.

B. BGL acts as a Data Processor

C. You wish to subcontract certain Services, which imply the processing of personal data to the Processor.

D. BGL and You seek to implement a data processing addendum that complies with the requirements of the current legal framework in relation to data processing.

E. BGL and You wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Addendum shall have the following meaning:

Addendum means this Data Processing Addendum and all Schedules;

Company Personal Data means any Personal Data Processed by the Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

Data Protection Laws means, to the extent applicable to the performance of the Services, the EU Data Protection Laws, UK Data Protection Laws and the applicable data protection or privacy laws of any other country;

EEA means the European Economic Area;

EU Data Protection Laws means the GDPR, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time;

GDPR means EU General Data Protection Regulation 2016/679 and, as applicable, the UK GDPR;

Services means online secure services provided by the Data Processor pursuant to the Principal Agreement;

Subprocessor means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the provision of the Services. BGL's Subprocessors are linked in Annexure C.

UK Data Protection Laws means the GDPR as transposed into UK law pursuant to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) ("UK GDPR"), the Data Protection Act 2018, and any other laws applicable the processing of personal data and privacy, in each case as amended, replaced or superseded from time to time.

1.2 The terms, **Commission**, **Controller**, **Data Subject**, **Member State, Personal Data**, **Personal Data Breach**, **Processing** and **Supervisory Authority** shall have the same meaning as in the Data Protection Laws, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than as set out in the Annex to this Addendum or otherwise on the relevant Company's documented instructions.

2.2 The Company hereby instructs Processor to Process Company Personal Data in connection with the performance of the Services and warrants that it has all necessary notices, consents and approvals in place to provide the Company Personal Data to the Processor and its Subprocessors for Processing in accordance with this Addendum.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with applicable laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 By accepting the Principal Agreement, the Company grants the Processor general authorisation to engage Subprocessors for processing Company Personal Data. The Processor will ensure that each Subprocessor is bound by data protection obligations that are at least comparable to those in this Addendum.

5.2 The Processor must carefully select Subprocessors, with particular attention to the suitability of their technical and organisational measures.

5.3 A list of Subprocessors is linked in Annexure C.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the Company obligations, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by applicable laws to which the Processor is subject, in which case Processor shall to the extent permitted by applicable laws inform Company of that legal requirement before the Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform the Supervisory Authority and/or Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall cooperate with the Company and take reasonable commercial steps as directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

9. Deletion or return of Company Personal Data

9.1 In accordance with this section 9, the Processor shall delete, and ensure the deletion of, all copies of the Company Personal Data after 12 months from the date of cessation of all Services involving the Processing of such data, or within any other time frame agreed upon.

9.2 The Processor may continue to store Company Personal Data to the extent required to comply with its legal obligations, including as required by Data Protection Laws or to the extent an exemption applies under Data Protection Laws.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information reasonably necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Processor.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Addendum does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law. Any audit shall be subject to reasonable prior notice and agreement as to the date and time and conduct of the audit, and may be subject to supervision by the Processor.

11. Data Transfer

The Processor will not transfer the Data outside of the European Economic Area (EEA) nor the United Kingdom (UK) unless it has taken such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Law. Such measures may include (without limitation) transferring the Data to a recipient in a country that the European Commission and/or the UK Secretary of State (as applicable) has decided provides adequate protection for personal data (for example, New Zealand) or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission and/or UK Secretary of State or UK Information Commissioner (as applicable). To this end, Company authorises the Processor to enter into standard contractual clauses with any recipient of Company Personal Data that is not located in a territory deemed adequate where this is necessary for the transfer of Company Personal Data for the proper performance of the Services.

12. General Terms

12.1 Confidentiality

Each Party must keep this Addendum and information it receives about the other Party and its business in connection with this Addendum ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 Notices

All notices and communications under this Addendum must be in writing and delivered personally, by post, or by email to the Processor's assigned account manager, or to updated addresses as notified by the Parties.

13. Governing Law and Jurisdiction

13.1 Subject to clause 13.2, this DPA is governed by the same laws as the same jurisdiction which governs the Principal Agreement.

13.2 To the extent required to comply with the GDPR and UK GDPR, and only in relation to matters relating to the compliance of this DPA or a party's actions under it in relation to GDPR or UK GDPR, this DPA shall also be governed by the laws of each Member State where EU Data Protection Laws and the UK Data Protection laws, as applicable.

13.3 Each party irrevocably submits to the jurisdiction described in clause 13.1 with respect to any disputes or claims however arising under this DPA.

Annexure A – Data Processing Schedule

Subject matter and duration of processing of personal data

The subject matter is the processing of personal data for the purpose of providing the Services and associated support.

Data processing will continue for the duration of the Principal Agreement, plus the period stipulated in the data processing addendum in accordance with clause 9.1.

Nature and purpose of processing personal data

The processing of personal data facilitates the provision and support of the Services as required under the Principal Agreement.

Types of personal data processed

The types of personal data processed include:

Type of personal data	Examples include
Names	First, Middle, Surname, Chinese Name
Other Names	Casual Name, Chinese Alias, Chinese Name, Other Name
Addresses	Residential, Business, Postal, Alternate, Correspondence, Service
Tax/Business Numbers	ABN (Australian Business Number), Tax File Number, Inland Revenue Department number, or any Other number that is defined as a Tax/Business number
Identification Numbers	Passport Number, Australian Director ID, Employment ID, SG FIN or any Other number that is defined as an Identification number
Professional ID Numbers	Agent number, Audit number, ID numbers of Professional Associations like Chartered Accountants, Certified Practicing Accountants, etc

Birth Details, Nationality, Gender	Date of Birth, Date of Death, Gender, Birth Country, Birth Place, Nationality
Communication Details	Email, Fax, Phone, Mobile, Skype
Occupations	Occupation details as defined
Relationships	Association like shareholdings, unitholdings, beneficiaries, membership with entities like companies or trusts
Directorships	Details where an individual is a Director of an entity
Online identifier	IP address, Cookie ID
Geolocation data	Location data
Biometric	Facial recognition data

Categories of data subjects

The categories of data subjects include:

a) employees of the Company

b) clients of the Company

c) individuals associated with clients of the Company

Annexure B - Technical and Organisational Measures

The Processor shall, at a minimum, implement and maintain technical and organisational measures to ensure the confidentiality, integrity, and availability of data, as outlined below.

Governance and Organisational Measures:

- Roles and responsibilities defined
- On-going training for employees
- Segregation of duties
- Contractually obligate all employees to maintain confidentiality and integrity of handling of personal data
- Contractually require suppliers and downstream API consumers to implement appropriate technical and organisational measures relative to the nature and scope of the information being processed
- Background screening of prospective employees
- Role-based access control
- Regular production user access reviews
- Password policy requiring minimum requirements

Risk Management and Compliance:

- Implementation of an Information Security Management System, as prescribed under ISO 27001
- Certification under ISO 27001
- Business Continuity Plan
- Implementation of disaster recovery plan and procedures

Technical Security Measures:

- Protection of web applications and databases using firewalls and load balancing
- Segregation of public and private networks by way of SASE
- Data Loss Prevention measures
- Physical access controls
- Encryption in transit and at rest
- Patch management
- Vulnerability scanning
- Endpoint malware scanning
- Static code analysis testing
- Code reviews
- Encryption key management and rotation

Operational Security:

- Regular maintenance of systems
- Regular backups
- Audit logs
- Security Information and Event Management system

Annexure C - Subprocessors

BGL (the “Processor”) engages certain Subprocessors to assist with the provision of services to You.

An up-to-date list of Subprocessors is available here.